UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

Case No. 21-CR-20264
Hon. Denise Page Hood

YLLI DIDANI,

Defendant.

Mark Bilkovic (P48855)	Wade G. Fink (P78751)
Assistant United States Attorney	WADE FINK LAW, P.C.
211 W. Fort St., Ste. 2001	550 W. Merrill St., Ste 100
Detroit, MI 48226	Birmingham, MI 48009
(313) 226-9623	(248) 712-1054
mark.bilkovic@usdoj.gov	wade@wadefinklaw.com
Attorneys for the United States	*Attorneys for Didani*

DEFENDANT'S SUPPLEMENTAL BRIEF
IN SUPPORT OF MOTION TO SUPPRESS

Defendant YLLI DIDANI, (hereinafter, "Didani"), by and through counsel, submits the following supplemental brief in support of his Motion to Suppress.[1]

[1] On October 19, 2022, Didani filed a Motion to Suppress Evidence and for Evidentiary Hearing. *See* D/E # 53. The Government timely answered on January 13, 2023. *See* D/E #65; D/E #62 (extending time to file answer). Didani timely replied on February 15, 2023. *See* D/E #70; D/E #69 (extending time to file reply). The Court ordered an evidentiary hearing on

I. THE EVIDENTIARY HEARING

Joshua Bianchi and the Genesis of the Investigation

Joshua Bianchi is an Intelligence Agent at the United States Border Patrol ("USBP"). Tr. at 8. From 2014 to 2017, he was assigned to a Homeland Security Investigations ("HSI") task force. *Id.* at 9. When Agent Bianchi was assigned to the HSI task force in 2014, it was to investigate cross-border gun crimes. *Id.* at 11-12. This morphed into an unclear assignment of "money laundering … drugs … just guns …cross-border criminal activity." *Id.* at 11. Then in 2017, Agent Bianchi's HSI task force became a "guns and gangs task force." *Id.* at 12. The vagueness of the task force carried into how cases were assigned. Agent Bianchi explained "either…your group supervisor would assign you a case or you could bring a case to the group from your home agency." *Id.*

---

the Didani's Motion to Suppress, which took place on April 24, 2023. *See* Minute Entry from April 24, 2023; *see also* Transcript from Evidentiary Hearing of April 24, 2023 (hereinafter, "Tr. at (page:line)") at D/E # 77. The Court invited supplemental briefs following the Evidentiary hearing, which, after multiple stipulations, were due to be filed July 3, 2023. Tr. at 293-295; *see* D/E # 78, 79, and 80 (extending time to file supplemental briefs). The Court will hold oral argument on August 2, 2023. *See* Minute Entry of June 29, 2023.

Agent Bianchi tried the latter, opening a "case" on Didani in 2015 "due to information that [Bianchi] received from the [USBP]." *Id.* This report, as did many thereafter, began with a sentence describing the investigation as being "related to the smuggling of marijuana between the United States and Canada and possible money laundering." *Id.* at 68:5 (February 2015 report); 74:19 (July 22, 2015 report); 80:2-5 (July 29, 2015 report).

Agent Bianchi claimed that Didani was part of a drug investigation dating as far back as 2008. According to Agent Bianchi, HSI and the Federal Bureau of Investigation ("FBI") were investigating a trucking company for allegedly moving marijuana and cocaine in and out of Canada. Agent Bianchi testified there was an informant implicating Didani. *Id.* at 30. On cross-examination, though, Agent Bianchi conceded to knowing little:

> [Defense Counsel]. And, without saying, do you know who that informant is?
>
> [Agent Bianchi]. No.
>
> Q. Did you look into the informant's background at all?
>
> A. No.
>
> Q. Do you know anything about the informant's veracity, their character for truthfulness?
>
> A. No.

Id. at 70.

The 2008 information being scant, Agent Bianchi testified that his opening report was also based on "information" from a 2013 incident where there was "suspicious information at a marina in St. Clair Shores, Michigan, that could have possibly led to drug or money smuggling back and forth between Canada and the U.S." *Id.* More specifically, Agent Bianchi testified, a "security guard at the marina called [USBP] stating there was (sic) individuals going out on jet skis taking off towards Canada, they were gone for a couple hours at a time, and then returning back." *Id.* at 14. Didani was not mentioned or involved in this incident. Two individuals named Eric Puzio and Vaughn Evasquez were. *Id.* at 15. Agent Bianchi conceded that he authored this report, titled "Didani's Opening Report," on February 9, 2015 and such report makes no mention of Didani at all. *Id.* at 66-67.[2]

But Agent Bianchi took an interest in Puzio. In fact, Agent Bianchi confirmed on cross-examination that the "genesis" of his investigation was

[2] Agent Bianchi confirmed on cross-examination that the 2008 information and connection to Eric Puzio were the only bases for this opening report in 2015. *Id.* at 72:25. It seems that it could not have been based on any information related to Hussein Hussein, discussed *infra,* because the information related to Hussein Hussein was not discovered until *after* the opening report was written. *Id.* at 72:14-16.

Puzio. *Id.* at 71:14. Puzio had previously been arrested for cocaine trafficking and gun charges. *Id.* at 16. Based only on this historical information, Bianchi opened a "[d]rugs and money laundering" investigation. *Id.* Agent Bianchi alerted law enforcement to Puzio's travels, such that if he traveled internationally, law enforcement would be notified. *Id.* at 17-18. On two occasions in 2014, Puzio made last minute reservations to visit St. Maarten in the Caribbean islands and only stayed for one evening. In addition, Puzio, several months later, Puzio traveled to Colombia. *Id.* at 18-19.

The trip to Colombia in August of 2014 (*id.* at 19) would turn out to be important - to Agent Bianchi, at least. The trip, which Agent Bianchi testified was suspicious because the reservations were made four days prior to the trip, and because the country is "a source of cocaine," included a travel companion for Puzio. That was Didani. *Id.* When Agent Bianchi looked further into the Colombia trip, he noticed that Didani flew into Colombia with Puzio, but returned alone the same day. *Id.* Puzio stayed for three or four days. *Id.* at 20. Agent Bianchi also noticed that the trip reservations were made by "Hussein Hussein." *Id.* at 20. Mr. Hussein was allegedly subject to a prior *arrest* (not conviction) for narcotics, was allegedly being investigated for "a large-scale narcotics" ring, and had previously come back into the

United States with "large amounts of money, cash." *Id.* at 21. In attempting to explain other suspicions related to Mr. Hussein, Agent Bianchi testified to a bizarre situation where a boat traveled from Canada to the United States with a vehicle on board that was registered to Mr. Hussein. *Id.* at 23-24. There was little explanation as to the illegality and no testimony about an arrest or charge. Agent Bianchi acknowledged that Didani was not involved. *Id.* at 83:19.

In 2014, Puzio and Didani traveled together to Albania. *Id.* at 24. Didani is an Albanian citizen and a United States as a permanent resident. *Id.* at 25. Looking further into Didani, Agent Bianchi found drunk driving convictions and an acquittal in a drugs and gun case. *Id.* at 26. He noticed Didani had multiple international reservations where he did not board the plane – two made flights and four missed flights over seven months. *Id.* at 26-27.

Based on the foregoing – the connection to Puzio and Hussein, and his travel habits – Agent Bianchi placed a travel alert for Didani, which would alert law enforcement that Didani was traveling in or out of the United States. *Id.* at 30. Agent Bianchi was notified that Didani would be flying into Chicago O'Hare on July 30, 2015. *Id.* at 31. He notified United States Customs

and Border Protection ("CBP") to set up an interview and traveled to Chicago O'Hare Airport to meet Didani personally.

Agent Bianchi testified that CBP Officer Fuentes conducted the interview at the secondary search area. *Id.* at 88:13-14. There was also another unknown CBP officer present. *Id.* at 32, 88. During the interview, Didani explained that he was always stopped at the border because of, what he believed to be, his drunk driving convictions. *Id.* at 33. CBP and Agent Bianchi questioned Didani about his living situation in the United States and his travel abroad. Didani was asked about his trip to Colombia the prior year. Didani explained he traveled to Colombia for a wedding, and that he was denied entry and had to return to the United States. *Id.* at 35. Agent Bianchi did not follow up with Colombian authorities and conceded that Didani could have been telling the truth. *Id.* at 100:1.

Agent Bianchi was determined to find Didani suspicious. Didani explained some of his travel, including going to Dubai for a Drake concert, which he corroborated by showing a picture of himself at the concert. *Id.* at 39. In discussing Didani's travels, though, even though Didani had not been proven untruthful, Agent Bianchi included a gratuitous reference in his report to the terrorist group Islamic State of Iraq and Syria ("ISIS") and an

attack that took place in Sanilurfa, Turkey around the time Didani was visiting. Even while acknowledging that he had "absolutely no[]" evidence to suggest Didani was involved in terrorism, he nevertheless permitted the inference in a federal report. *Id.* at 101.[3]

Didani also discussed with law enforcement his coal business in Albania, trucking business in Michigan, and connection to Puzio. *Id.* at 37. Agent Bianchi, on hearsay and without exhibits, testified that these explanations were lies based on some alleged research he had done. *Id.* Agent Bianchi was suspicious, as well, because apparently Didani did not produce business cards, hotel information, or names of associates of his, all related to the coal business. *Id.*

Agent Bianchi testified that during the interview, Didani was scrolling through his iPhone "trying to prove his point that he was doing certain things." But while showing these pictures, according to Agent Bianchi, Didani showed law enforcement a picture of "Adriatic Sheko," who the agent believed was one of the individuals associated with a trucking

[3] Agent Bianchi acknowledged he knew nothing of the attack, did not know ISIS was typically carried out in the name of Islam, did not know Didani is not Muslim, did not know it bordered Syria, did not know the target of the attack, and more. *Id.* at 102-104.

company being investigated for drug smuggling back in 2008 (for which he had also implicated Didani based on an unknown, undisclosed, untested informant). *Id.* at 40. Agent Bianchi could not tell the Court if Sheko had any prior arrest, convictions, or criminal history whatsoever, but conceded if there were, he "normally" would have added it to his report, which he did not here. *Id.* at 111-112.

CPB Officer Fuentes conducted a manual search of Didani's phone. *Id.* at 40-41. While scrolling through photographs, Agent Bianchi testified he saw a picture of an AR-style rifle, as well as pistols and large amounts of money wrapped in cellophane. *Id.* at 41. To Agent Bianchi, this indicated "cross-border criminal narcotics activity." *Id.* And because Agent Bianchi was "trying to make it so Didani did not miss his connecting flight," law enforcement did a forensic extraction of Didani's phone. *Id.* at 41:23-25. According to Agent Bianchi, this means "produce a copy of what's on the phone onto another media device that you can look at" later. *Id.* at 95:23-24. Didani was detained by law enforcement for "[f]ive or six hours," according to Bianchi. *Id.* at 112:18. He was not free to leave at any point. *Id.* at 112:21.

The Warrantless Search of Didani's Phones for Over a Year

Agent Bianchi reviewed the forensic extraction from Didani's phone without a warrant. *Id.* at 43, 96. He allegedly saw narcotics, guns, and currency, including a gun next to a cocaine and money. *Id.*[4] He also noticed "shipping containers, shipping lines, like they were researching ways to ship things…international[ly]." *Id.* In reviewing Government's Exhibit 4, Agent Bianchi described "eight stacks" of cash and in Government's Exhibit 5, large amounts of currency in a black duffel bag. *Id.* at 47.

Agent Bianchi had been referring to his investigation of Didani as "related to the smuggling of marijuana between the United States and Canada and possible money laundering." *Id.* at 68:5 (February 2015 report), 74:19 (July 22, 2015 report), 80:2-5 (July 29, 2015 report). But he switched to description of the investigation to: "information regarding possible smuggling of steroids, contraband, vehicles, possible counterfeit money, and money laundering." *Id.* at 90:2-6. When asked the reason the investigation became so much more expansive in scope, Agent Bianchi answered: "that would be his cellphone." *Id.* at 91:13. He was referring to viewing the digital

[4] Pictures from the interview and post-interview search of the forensic copy were admitted as Government Exhibits 1 through 5. *Id.* at 44-46.

copy of Didani's cell phone after Didani had been admitted to the United States and away from the border. He testified that over a year's time, he viewed thousands of pictures on Didani's phone and admitted that he searched the contents of Didani's *entire cell phone,* "thoroughly go[ing] through the phone," searching "every corner of it." *Id.* at 107. This included text messages from different applications on the phone. *Id.* at 106-107. This included searching every application on the phone "that was available." *Id.* at 107.

While surveilling Didani after the July 30, 2015 encounter, Agent Bianchi acknowledged that "the photographs and text messages and things that [Agent Bianchi] viewed on Mr. Didani's phone [] heighten[ed his] suspicions about these otherwise innocuous activities." *Id.* at 129:3-7. Agent Bianchi was more suspicious of Didani's activities "[b]ecause of the images and messages that were on the phone." *Id.* at 129:10. When asked if there was "anything else from [a] report . . . or at this time [September of 2015] generally … to call to the Court's attention…", Agent Bianchi answered: "No." *Id.* at 131:17.

For the first time on cross-examination, never mentioned on direct examination, Agent Bianchi recalled several wire transfers amounting to

$23,000.00 coming form an individual Don Larsen, allegedly benefitting Didani. *Id.* at 138. Agent Bianchi provides no evidence or detail as to how these funds were associated with Didani, or why they were illegitimate. *Id.*

At this point, Agent Bianchi agreed that his suspicions of Didani amounted to the following: money transfers from Don Larsen, connection to Eric Puzio, connection to Hussein Hussein, and the phone he searched after his encounter with Didani in July of 2015. *Id.* at 140-141. These were the "premise" of his suspicions leading up to a second encounter the following year. *Id.* There was nothing he wanted to add. *Id.*

A year after the first encounter in July of 2015, in August of 2016, Agent Bianchi received an alert that Didani was flying into the United States again via Chicago O'Hare Airport. *Id.* at 55-56. Didani was allegedly flying through the United States to Mexico City. *Id.* at 56. Agent Bianchi testified that Puzio was also traveling to Mexico from Detroit. *Id.* On August 6, 2016, Agent Bianchi contacted HSI Special Agent ("SA") Daniel Nugent. *Id.* at 57. Agent Bianchi gave SA Nugent background information and requested that SA Nugent conduct a seizure, search, and interview of Didani. *Id.* After the interview of Didani, SA Nugent contacted Agent Bianchi to tell him he had

detained two of Didani's cell phone and he would be sending them to Agent Bianchi. *Id.* at 146:17-19.

CBP Officer Matthew Parisi and the August 2016 Interview

Matthew Parisi is a CBP Officer. He has been an agent for 11 years and was assigned to Chicago O'Hare Airport in 2014. *Id.* at 189. He explained that on August 6, 2016, he was assigned to Didani as a "lookout" for the day, meaning he is to stop a passenger at the plane and escort them to border inspection for a border search. *Id.* at 199-201. Officer Parisi did not specifically recall Didani. *Id.* at 201:3. But he testified as to his general practice. *Id.*

Officer Parisi testified that once a person has been positively identified, two CBP officers would meet the person at their plane, and "take their passport [and] cellular device." *Id.* at 202:13-14. Based on his general practice, Officer Parisi stated next the passenger and agents go through primary inspection, retrieve luggage, and proceed to the secondary inspection area. *Id.* at 206:21-24.

Officer Parisi testified that Didani declared, prior to any search, that he was in possession of human growth hormone. *Id.* at 208:24. Officer Parisi stated that Didani made this declaration before he was to be searched. *Id.* at

230:11. He could have made it on the declaration form on the airplane, to the primary officers, or at any time prior to the search. Officer Parisi could not say for sure. *Id.* at 230: 18. Ultimately, he agreed that Didani was not trying to hide the HGH. *Id.* at 231:4. Officer Parisi did not know if the substance was legal in other countries that Didani traveld to. *Id* at 231:7-10.

Officer Parisi and his CBP partner, Officer Leeker, were present for this encounter. *Id.* at 238:20-21. Officer Parisi recalled both himself and Officer Leeker being present because "there's always somebody present during the inspection." *Id.* at 211:8. And, he clarified that because he was on a certain unit, "it would have only been [Officer Parisi] and Officer Leeker" with Didani. "Nobody else." *Id.* at 238:19-21.

Officer Parisi testified that he found steroids and also detained two phones that belonged to Didani – a blackberry and iPhone. *Id.* at 218. He testified that "[b]ecause of our agreement with HSI, any time we find an illegal substance we have to make notification to HSI. HSI responded. The phones were then transferred over to HSI." *Id.* at 218:12-14. According to Officer Parisi, SA Nugent arrived to take custody of the phones.

Daniel Nugent and Didani's Cell Phones in 2016

Daniel Nugent is the special agent in charge of the Chicago O'Hare Airport for HSI. *Id.* at 260:16-17. He worked for CBP before HSI. *Id.* at 260:23-24. SA Nugent was informed by Agent Bianchi that Didani was being investigated for drugs and was scheduled to arrive at O'Hare Airport on August 6, 2016. *Id.* at 263-264. He was asked to send Didani to secondary inspection. *Id.* SA Nugent arrived after the interview with Didani and took two cell phones into his possession. *Id.* at 265-266.

SA Nugent stated that he did a "brief search" of photographs in one of the phones. *Id.* at 266:21-23. SA Nugent stated that he discovered "a hand-drawn picture of what appeared to be a cargo container with a raiser floor and an arrow pointing [] to the raised floor." *Id.* at 267:3-7. SA Nugent said this was significant because in his experience "drug smuggling occurs inside of cargo containers with raised floors." *Id.* at 267:13-15. After viewing this image, SA Nugent stopped searching the phone because he "saw what may have been evidence of a crime." *Id.* at 270:3-4. But SA Nugent also claimed to have been searching the phone "looking for . . . merchandise relating to HGH" and "perhaps pictures of drugs…" *Id.* at 277. He further testified that he was actively looking for "evidence of a crime," including, "drug

smuggling and drug distribution" because Didani "was under investigation" for both." *Id.* at 283-284.

II. ARGUMENT

A. The Warrantless Copying and Searching of a Cellular Phone is Unconstitutional Post-*Riley v. California*

On May 11, 2023, Southern District of New York Judge Jed S. Rakoff decided *United States v. Smith*, Case No. 22-cr-352 (SDNY 2023) (Opinion and Order Denying Motion to Suppress) (attached as **Exhibit A**). The Court held, in no uncertain terms:

> Applying this balancing framework to phone searches at the border yields the same result as in *Riley*.[5] None of the rationales supporting the border search exception justifies applying it to searches of digital information contained on a traveler's cell phone, and the magnitude of the privacy invasion caused by such searches dwarfs that historically posed by border searches and would allow the Government to extend its border search authority well beyond the border itself. **As such, the Court concludes that the Government may not copy and search an American citizen's cell phone at the border without a warrant absent exigent circumstances**.

[5] *Riley v California,* 572 U.S. 373 (2014).

Id. at 8. For the reasons discussed herein, and because the Sixth Circuit has not held otherwise citing *Riley,* this Court should conclude precisely the same and find there was a Constitutional violation in this case.

As this Court is aware, pre-*Riley,* the Sixth Circuit explained that "searches of people and their property at the borders are per se reasonable, meaning that they typically do not require a warrant, probable cause, or even reasonable suspicion." *United States v. Stewart,* 729 F.3d 517, 524 (2013). Our Supreme Court wrote that the "Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004). But there comes a point where a search becomes too attenuated from the border, such that the "extended border doctrine applies," essentially meaning that once a person has cleared the border, he regains *some* expectation of privacy and therefore varying degrees of suspicion are required for continued search. *Stewart,* at 525 (collecting cases from other circuits).

Riley was and is a gamechanger. Much of the authority cited by the Government is either pre-*Riley,* or uses rationale that is incompatible with *Riley.* In *Riley,* a 9-0 ruling of the Supreme Court delivered by Chief Justice Roberts and joined by an ideological gamut spanning Justice Ginsburg to

Justice Thomas, the Supreme Court faced the question of "whether police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested" pursuant to the search-incident-to-arrest exception to the Fourth Amendment. *Riley,* at 381. *Riley* combined two cases involving defendants who were properly arrested and had police seize their respective cell phones from their person. In both cases, police, one hours later, one minutes later, searched through the cell phone without a warrant and discovered evidence in pictures and text messages of other crimes.

The defendants brought a motions to suppress. The Supreme Court reviewed the purpose and history of the search-incident-to-arrest exception to the warrant requirement. *Id.* at 382. The justifications for the exception were the need for a bright-line, clear rule with regard to searching a person for **weapons** or **evidence** of the crime for which he or she is arrested. *Id.* at 384. The Supreme Court explained it previously held that when someone is lawfully arrested upon probable cause, categorically, their person may be searched. *Id.*

However, this left open the question of what extent modern cell phones could be searched incident to arrest given the "vast quantities of

personal information literally in the hands of individuals" and the "little resemblance [a phone has] to the type of brief physical search considered" in previous incident-to-arrest cases. *Id.* at 385. The most important question in this situation is as follows: whether the application of the exception to a particular category of search would "untether the rule from the justifications underlying [it]." *Id.* at 386 (citing *Arizona v Gant* 556 U.S. 332 (2009)).

In *Riley,* the Court found that permitting police officers to rummage through the vast data in a cell phone incident-to-arrest would indeed untether the rule from its justifications and therefore was unconstitutional without a warrant because digital data could not be used as a weapon and the concern over the destruction of evidence is lessened once the cell phone is seized (and airplane mode-like methods can be employed to prevent remote deletion of data). *Id.* at 388-389.

The part of *Riley's* analysis that is particularly important here, and in Judge Rakoff's Opinion and Order, is the incident-to-arrest exception's reliance on a reduced privacy interest of the arrestee. *Id.* at 391. A person lawfully arrested for a crime has diminished privacy interests in the items on his person or within his reach. *Id.* But when the government said the same is true for the contents of a cell phone, the Supreme Court rightly rejected

the argument, stating "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." *Id.* at 393. And it differs in ways both "quantitative and qualitative" because modern cell phones are "minicomputers . . .[with] immense storage capacity…[and] the possible intrusion on privacy is not physically limited in the same way" it is with physical items. *Id.* at 393-394. At the time, the best selling cell phones had "a standard capacity of 16 gigabytes)" (*id.* at 394) – now, cell phones have standard capacity ranging from 64 gigabytes to *one full terabyte* in the palm of one's hand.[6]

Thus, the sheer amount of data and private information that is contained on a person's cell phone is "the sum of an individuals' private life," which "can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions." Further, "[m]obile application software . . . can form a revealing montage of the user's life." This makes storage devices like cell phones materially different from the searches anticipated by the incident-to-arrest exception.

> Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in

[6] The lowest available storage capacity for Apple's newest iPhone is 128 GB. *See* https://www.apple.com/shop/buy-iphone/iphone-14

> digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.

Id. at 397.

With this backdrop, Judge Rakoff decided *Smith. See* **Ex. A.** In *Smith,* HSI and FBI were investigating the defendant for a fraud conspiracy involving government contracts. HSI and FBI asked CPB to detain the defendant when he returned from Jamaica to the United States. *Id.* at *2. Using passcodes provided by the defendant, HSI agents made a forensic copy of the defendant's phone, returning the original to the defendant, and admitting him into the United States. *Id.* at *3. Searching the forensic copy without a warrant, the government found substantial evidence of the fraud *and* additional crimes, like gang activity. After 38 days, the government applied for a warrant and received one. *Id.* The defendant brought a motion to suppress.

The District Court, citing *United States v Ramsey,* 431 U.S. 606, 616 (1977), first discussed the purpose of the border search exception – "the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country are reasonable simply by

virtue of the fact that they occur at the border." *Id.* at *4. The Court also noted varying degrees of suspicion sometimes required at the border. *Id.*

Judge Rakoff opined, as this Court should, that *Riley's* "logic would seem to apply to cell phone searches at the border." *Id.* at *6. And applying the same question from *Riley*, this time asking whether the justifications underlying the *border search exception*, rather than the incident-to-arrest exception, yields the same result: permitting warrantless copying and searching of cell phones seized at the border untethers the border search exception from its justification. *Id.* at *7. Judge Rakoff reasoned that the border search cases rely on the governmental interest in protecting the integrity of the border, including preventing illicit substances and persons who pose a threat (diseases, narcotics, explosives, etc.) *Id.* at *7. But interdiction of contraband or dangerous persons cannot be accomplished by stopping a cell phone, as data does not just exist on the cell phone. You cannot interdict and stop the data from entering. The Court concluded, therefore, that law enforcement cannot search a cell phone at the border. *Id.* at *9.

This Court should conclude the same way and hold that a warrantless copying and searching of a cell phone is unreasonable under the Fourth

Amendment in light of *Riley*. *Id.* at *11. Under that rule, the 2015 search was unlawful and everything thereafter are fruits of the poisonous tree.

In this case, Agent Bianchi testified that after copying Didani's cell phone in 2015, without a warrant, he "thoroughly" searched the phone, "every corner of it." Tr. at 107. Over more than a year's time, from July of 2015 through August of 2016, Agent Bianchi made use of the image made of Didani's cell phone to look into every part of his life. This included text messages from different applications on the phone. *Id.* at 106-107. This included searching every application on the phone "that was available." *Id.* at 107.

> [Defense counsel]: So, to be clear, based on what the government will argue, I'm not saying it's necessarily wrong, but just to be very clear for the record, you did a warrantless search of the entire phone that he had on him July 30 of 2015? And there may be an exception to that. I'm asking you just to make it very clear on this question. You did a warrantless search of his phone on July 30, 2015 through August 2016. Yes?
>
> [Agent Bianchi]: Yes, Sir.

Id. at 108:15-24 (cleaned up).

From the time Agent Bianchi wrote Didani's opening report in February of 2015, through his reports written prior to Didani's first stop on

July 30, 2015, Agent Bianchi had been referring to his investigation of Didani as "related to the smuggling of marijuana between the United States and Canada and possible money laundering." *Id.* at 68:5 (February 2015 report), 74:19 (July 22, 2015 report), 80:2-5 (July 29, 2015 report). But Agent Bianchi changed this description after searching Didani's cell phone, writing that the investigation was now concerning "information regarding possible smuggling of steroids, contraband, vehicles, possible counterfeit money, and money laundering." *Id.* at 90:2-6. Agent Bianchi concedes this is the first mention of steroids, contraband other than marijuana, vehicles, and counterfeit money. *Id.* at 90-91.

And, critically, Agent Bianchi candidly told us why his investigation changed: "that would be his cellphone." *Id.* at 91:13.[7] That is chilling. Agent Bianchi unabashedly admitting that for a year's time he made use of extraordinary amounts of data, without a warrant, hundreds of miles from the airport, Didani having been admitted into the country, to further a

[7] Agent Bianchi added "vehicles" to the investigation because he saw pictures of "multiple cars, high-end cards, and also titles of other people that are not in (sic)." *Id.* at 93:20-21. He added steroids to the investigation, as allegedly having viewed it on his phone. He testified that there we thousands of pictures. *Id.* at 105-106.

criminal investigation that had nothing to do with the border. Without a warrant, Agent Bianchi rummaged through Didani's life, accessing more information about him that he would have found in his home.

Agent Bianchi made use of the extensive search of Didani's phone to further his investigation. And in September of 2015, a little over a month after the first airport encounter, Agent Bianchi wrote that he had reviewed suspicious text messages in 2014 about money being owed. *Id.* at 126-127. In that same report, Agent Bianchi detailed surveillance of Didani. *Id.* at 128. He did not view Didani do anything illegal, but acknowledged that "the photographs and text messages and things that [Agent Bianchi] viewed on Mr. Didani's phone [] heighten[ed his] suspicions about these otherwise innocuous activities." *Id.* at 129:3-7. Stated another way, Agent Bianchi was more suspicious of Didani's activities "[b]ecause of the images and messages that were on the phone." *Id.* at 129:10. When Didani boarded a plane by himself, and takes bags out of a trunk of a car, "the money, the guns, and" the other things on his phone give different meaning to this observed conduct. *Id.* at 129:15.

Judge Rakoff's conclusion as it relates to the border search exception and *Riley* is the logical mandate in order to be faithful to *Riley*. And while

Judge Rakoff acknowledged multiple Circuits who have held differently,[8] these Circuits disregard the central reasoning in *Riley* by failing to appreciate the difference between tangible items and data. Cell phones are not capable of holding contraband – they don't physically hold drugs or guns. So, the only basis for searching a cell phone would be to look for evidence of a crime. That requires a warrant. *See Cano, infra,* at 1018. The government's interest in stopping crime is different from the government's interest at the border – which is to stop physical contraband or unwanted persons and items.

Judge Rakoff's conclusion also makes more sense practically, too, because a bright line rule, a categorical approach, makes it easier for law enforcement. In this case, law enforcement had no clue what the state of the

[8] *See, cf., Alasaad v. Mayorkas,* 988 F.3d 8, 21 (1st Cir. 2021); *United States v. Touset,* 890 F.2d 1227, 1235 (11th Cir. 2018); and, *United States v. Xiang,* 2023 U.S. App. LEXIS 11027 (8th Cir. May 5, 2023). But *see* Dissent in *United States v. Vergara,* 884 F.3d 1309 (11th Cir. 2018) ("To be sure, forensically searching a cell phone may lead to the discovery of physical contraband. A drug smuggler's deleted text messages, for example, may reveal the location of drugs inside the border. But this general law enforcement justification is quite far removed from the purpose originally underlying the border search exception: "protecting this Nation from entrants who may bring anything harmful into this country." *Id.* Excepting forensic cell phone searches from the warrant requirement because those searches may produce evidence helpful in future criminal investigations would thus "untether the rule from [its] justifications." *Riley*, 134 S. Ct. at 2485 (internal quotation marks omitted)).

law was, what was permitted and what was not. For example, when asked to explain why he sought a search warrant in 2016, but not in 2015, Agent Bianchi answered: "It was more due to the criminal activity that we thought was on the 2016 phones." *Id.* at 152:23-24. But that answer changed a few moments later, when Agent Bianchi testified, "we have border search authority so I don't need a warrant. I just need reasonable suspicion." *Id.* at 153:11-12. That was later amended, too, when discussing the 2016 warrant: "Because I wanted - - after what we had saw, we did do that. After what we saw on the phone, we did a search and seizure warrant." *Id.* at 153:17-19. A fourth answer was given, as well: "This is – suggestion is mostly because if you are doing a border search you are returning the item back to the person. This was not returned back to them." *Id.* at 153-154. This confusion was evident with all witnesses. Officer Parisi from the CBP did not know the difference between a "routine" and "nonroutine" search. Tr. at 241. SA Nugent testified:

> I believe at that time -- there's been so many changes to the border search law relating to electronic devices, but if I'm not mistaken I may have been told at some point around then that if you find evidence of a crime that the wise thing to do would be to stop searching, and that's what I did. I stopped searching, and I sent it up to the investigating agent for them to

> make a determination on what they wanted to do next.

Tr. at 281.

Judge Rakoff's approach makes this easy – if you want to search a forensic copy of an electronic storage device, such as a phone, you must get a warrant.[9] This protects the evidence by copying it in the same fashion it is stored at the time, which lessens concerns about its destruction. This protects the individual's privacy rights in that a neutral magistrate has to approve a substantial intrusion in your life.[10]

B. The Searches of Didani's Phones Were Unconstitutional Under Any Standard, Pre- and Post-*Riley*

Even if the Court is not inclined to adopt Judge Rakoff's holding, the analysis is similar even under other border search jurisprudence. Because

[9] The discussion in Section B.iii below applies equally to why this Court should adopt Judge Rakoff's rule.

[10] In addition to the more categorical approach, Judge Rakoff concluded that manual scrolling through cell phones at the border was, too, unconstitutional. This occurred in this case, as well, both in 2015 and 2016. Agent Bianchi, Officer Parisi, and SA Nugent all acknowledge manually searching the phone, finding evidence of what they suspected was a crime, and did so without a warrant. By doing so, under *Smith,* they violated the Fourth Amendment for this reason, as well.

law enforcement lacked individualized suspicion, the searches of Didani's cell phones in both 2015 and 2016 were unconstitutional.

The Supreme Court, pre-*Riley,* held that searches performed at international borders do not generally require a warrant, probable cause, or reasonable suspicion. *Ramsey, supra,* at 617-619. But the Supreme Court clarified in *Flores-Montano, supra,* at 152 that this authority is not unfettered and that "highly intrusive" border searches require at least reasonable suspicion. It was in *Flores-Montano* that the Supreme Court opened the door to "routine" versus "nonroutine" searches – the latter being more intrusive and requiring individualized suspicion. *Id.* The Sixth Circuit has not addressed the precise issue of "nonroutine" versus "routine," however, it has suggested reasonable suspicion applies in "extended border search[es]." *See United States v McGinnis,* 247 Fed. Appx. 589 (6th Cir 2007). The majority of courts, as well as the government in its answer (ECF No. 65 at PageID.463-464), agree that such a distinction was the mandate of *Flores-Montano.* This includes Judge Leitman in this our District (*see* Gov't Answer at ECF No. 65, PageID.464).

United States v. Aigbekaen, cited by Judge Rakoff, is illuminating on the question of these nonroutine searches. 943 F.3d 713 (4th Cir. 2019). While it

was decided post-*Riley,* it does not go as far as Judge Rakoff, but takes a middle position. The Fourth Circuit provides that forensic searches of a phone "must be treated as nonroutine border search[es], requiring some form of individualized suspicion." *Id.* (citing *United States v Kolsuz*, 890 F.3d 133 (2018)). More specifically, "to conduct such an intrusive search" into a cell phone without a warrant, "the government must have individualized suspicion of an offense that bears some nexus to the border search exception's purposes of protecting national security, collecting duties, blocking entry of unwanted persons, or disrupting efforts to export or import contraband." *Id.* at 721. Applying this standard, in *Aigbekaen,* citing *Riley,* the Fourth Circuit held that law enforcement's search of the defendant's electronic devices for child pornography, given his prior crimes, lacked the requisite nexus to the border search exception's rationale. *Id.*

i. No Individualized Suspicion Before 2015 Copying and Searching Didani's iPhone

In this case, there was inadequate individualized suspicion that criminal activity was afoot under any standard when Didani was stopped in 2015. Agent Bianchi copied and reviewed every aspect of Didani's iPhone, for an entire year, to build an ordinary criminal case, without a warrant. This level of intrusion was not justified by the border search exception.

As the Court reviews the hearing transcript, it will notice that sufficient legal suspicion of criminal activity by Didani, pre-2015, is virtually non-existent. And be there no mistake, the government itself thinks what came *after* the 2015 copying and searching of Didani's phones is what gave rise to clear reasonable suspicion, as it writes:

> Here, the images of firearms and bulk, banded currency, along with evidence of the movement of money initially found on Didani's iPhone in 2015, single handedly satisfy the reasonable suspicion threshold.

See ECF No. 65, PageID.465. So, if the 2015 forensic copying and searching of Didani's cell phone was unlawful, so, too, will be the 2016 search and the warrant requested more than a year later, as the fruit of the 2015 violation.

With regard to reasonable suspicion pre-2015, the Government believes there was adequate reasonable suspicion based on the following: (1) "11 Mile Boat Launch"; (2) Didani's association with Eric Puzio; (3) Didani being booked on a flight to Colombia by Hussein Hussein; (4) Hussein Hussein's activities on the Detroit River; (5) Didani's' having returned from Colombia on the same day as he traveled there; and, (6) Didani's four missed flights over seven months. That's it. The rest of the individualized suspicion

described by the Government is derived post-2015 search of Didani's phone. *See* ECF No. 65, PageID.466.

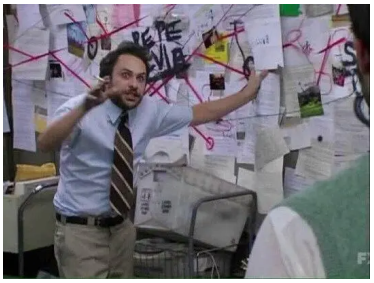
Breaking down this purported individualized suspicion, Agent Bianchi's testimony makes the Government's position untenable. First, the "11 Mile Boat Launch" and Mr. Hussein's activity on the river. Agent Bianchi plainly testified he had no evidence of Didani's connection to any of the suspicious activities on the Detroit River.[11] Tr. at 83:19 (Didani not involved in Hussein Hussein's river activities), 83:25 (Didani not involved in Puzio's jet ski river activities). Second, Didani's return from Columbia on the same day as his travel *to* Columbia. Agent Bianchi testified he never followed up with Colombian authorities as to whether Didani was admitted to the country, making an equally plausible explanation that Didani was not permitted entry into Columbia. *Id.* at 99:17. There is also a suggestion that traveling to Columbia, in and of itself, is suspicious. Does that mean the 4 million Columbian tourists, per year, are subject to searches of their entire life because of their chosen vacation?

[11] And even if he was connected somehow, we still know *nothing* about these incidents. Agent Bianchi's testimony did not explain how any of these river activities involving boats and jet skis and vehicles are relevant to anything. *See* discussion at ECF No. 70, PageID.496.

Those "suspicions" being so flimsy, where does that leave us? Missed flights and guilt by association. And "guilt by association" is not a basis "for reasonable suspicion to support a *Terry* stop." *Trice v United States,* 849 A.2d 1002, 1006 (D.C. Cir. 2004); *see also United States v. McGinnis, supra,* (6th Cir 2007) ("guilt by association does not itself suffice to establish the reasonable suspicion necessary to seize and search an individual who already has passed through customs…"). Agent Bianchi, throughout his testimony, piles inference upon inference, trying to connect Didani to other people and their alleged, albeit unexplained previous indiscretions, as somehow being relevant to Didani being a criminal.[12]

Agent Bianchi agreed that he merely had a "hunch." Tr. at 128:4. And that is precisely what the "individualized suspicion" was prior to 2015, it was "nothing more than a hunch without an articulable basis. It [never rose]

---

12 

The popular meme showing a conspiracy theory from the TV show "It's Always Sunny in Philadelphia" comes to mind. It is almost quite literally what the reasonable suspicion was at this point – pins and string connecting Didani to people who may or may not have engaged in some sort of vague criminality in the past.

above the level of guilt by association." *Kebe v. Brown*, 161 F. Supp. 2d 634, 641 (MD 2001). And even indulging the guilt by association desires of the Government, Agent Bianchi made clear throughout his testimony he was not even really sure what Mr. Hussein had ever done. *See* Tr. at 80:24 (Asked whether Hussein was convicted of any crime, Agent Bianchi answered, "I do not know). Agent Bianchi opened his file on Didani because of Didani's travels with Puzio that was booked by Hussein and because of some informant, who Agent Bianchi did not know or test the veracity of, in 2008. *Id* at 72:25. Those were the only things that formed the basis to open an investigation into Didani 6 months before he was stopped in July of 2015. *Id.* at Tr. 73:3.

For the Court to find reasonable suspicion justifying the 2015 warrantless copying and searching of Didani's phone, it would have to conclude that Didani's associations and missed flights are enough. If this justifies *Terry* stop, such that law enforcement can search through your entire life on your cell phone, then truly "anything goes" at the border. *United States v. Seljan,* 547 F.3d 993, 1000 (9th Cir. 2008) (en banc) (the government's interest in securing the border does not mean that "anything goes").

ii. No Individualized Suspicion for the 2016 Search and Seizure

In conjunction with, and independent of, the 2015 search and seizure, the 2016 encounter and subsequent search was likewise unconstitutional.

To be sure, the conduct was not somehow sanitary because in 2016 law enforcement decided to get a warrant. Agent Bianchi searched the phones, *again,* without a warrant:

> [Defense counsel]: So did you review the phones before you obtained the warrant on August 17, 2016?
>
> [Agent Bianchi]: Yes. They were searched, border-searched.
>
> Q: Okay. So between August 6 and August 17th using the border search exception there was warrantless entry into the two cellular phones that were seized before a warrant was obtained 11 days later. Is that what you just testified to?
>
> A: That is correct.
>
> ***
>
> Q: And then once you realized that there was bad stuff or criminality on that phone, you decided to apply for a warrant on August 17, 2016?
>
> A: With other circumstances, yes.

Tr. at 154-155. In addition, Agent Bianchi was indifferent towards getting a warrant, testifying multiple times he did not need one. *See, e.g.*, Tr. at 155:14 (testifying he has authority to search the phone without a warrant).

To conduct the manual and 11 days of warrantless searches of Didani's cell phones in 2016, the government relies on what it found in the 2015 warrantless searches of Didani's phone. That, in itself, is the fruit of the poisonous tree. But even independently, currency and firearms are not illegal. *See* Didani Reply at ECF No. 70, PageID.498-499.

iii. Both Searches of Didani's Phones Were Untethered from the Border Search Exceptions Justification

Regardless of the level of suspicion, the searches in both 2015 and 2016 were not justified by the border search exception's rationale. If this type of warrantless intrusion is permitted, without a warrant or proper connection to the border, it will subject many innocent individuals to embarrassing, harassing, unconstitutional intrusions into every aspect of their lives.

Of course, the Court is well-aware that Fourth Amendment analysis is not a results-oriented endeavor. Because the way our system is, this Court rarely, if ever, in a criminal case, has opportunity to see the folks that were unconstitutionally harassed by law enforcement and never hailed into the

criminal justice system. That is the idea behind suppression – a prophylaxis. It has become clear, through this case, and through the testimony at the hearing, that law enforcement is merely using its border search authority as a subterfuge to conduct full-scale criminal investigations and access information they otherwise would not be able to. And *that* untethers the border search exception from its justification. *Gant, supra.*

The justifications underlying the border search exception are fairly well-defined: "the protection of the integrity of the border." *United States v. Montoya de Hernandez,* 473 U.S. 531, 541 (1985). This includes denying entry to persons who lack authorization to be in the country, ensuring customs taxes are paid, and keeping out diseases, narcotics, and explosives. *See Martinez-Fuerte,* 428 U.S. 543, 556 1976; *Ramsey, supra*, at 616; *Montoya,* at 544. As Judge Rakoff summarized, at bottom, the government's interest is stopping unwanted persons and items from entering the country *at the border*. *Smith, supra,* at *8.

This interest is minimal, if it exists at all, once someone clear the border. Sure, interdiction of drugs at the border, discovery of items for which tax is due, and prevention of someone from entering the country, these are all things that at least have some nexus to the border search exception's

rationale. But seizing and/or copying a data device, only to let the individual and his luggage enter the country, and then spend the following days, months, and years intruding into that person's entire life through their cell phone is using a machete where a scalpel is required.[13]

Weighing the purported governmental interests against the privacy rights of an individual like Didani's privacy interests, applying the border search exception to the conduct here in 2015 and/or 2016, would untether the rule from its justifications. *See Ganta, supra.* As addressed herein, cell phones contain enormous amounts of information about an individual's life – communications, proof of their physical movements, financial transactions, internet searches, medical information, intimate photographs, and more. Didani does not contest that "an individual who presents [himself] at a border crossing has diminished privacy interests" in his belongings, just like the person who is arrested and taken into police custody has lessened expectations of privacy (*Riley*). But that has almost always been

[13] Arguments have been made and discussed here and in prior briefing about stopping "digital contraband." Among the other arguments discussed, such is in *Aigbakean,* and as Judge Rakoff logically points out, data exists elsewhere, on other devices, not just on the cell phone seizure. *Smith,* at *8. The government is not stopping this contraband from coming into the country, they are merely using the concept as an excuse to do a criminal investigation without a warrant.

a reduced expectation in tangible items. Cell phones, in contrast, carry more information than you would find in someone's home. *See Riley,* at 397. No traveler expects to forfeit *all* of their privacy "simply by carrying a cell phone when returning home from an international trip." *Smith,* at *9.

The governmental interests that underlie the border exception, therefore, cannot support the warrantless copying Didani's cell phone for searching *over a year's time* in 2015, and the warrantless seizing of Didani's cell phones in 2016 and searching for 11 days prior to obtaining a warrant. Nor can those interests justify such an intrusion at whatever amount of suspicion the government had here. Here, Didani was admitted to the United States in 2015, leaving behind a forensic copy of his cell phone. But once he was admitted – and the days, months, and year went by – the continued searching of his cell phone was no longer about the integrity of the border, it was about building a criminal case against Didani. And a general criminal investigation, even if noble or correct, is "unmoored" from the border search exceptions' justification. *See Aigbakean, supra* (Fourth Circuit holding that search for child pornography at border unrelated to border crimes).

HSI and CBP were targeting Didani in a general criminal investigation. Tr. at 242-243. As the Ninth Circuit explained: "warrantless searches of cell phones" are limited "only to determine whether the phone contains contraband." *See United States v. Cano,* 934 F.3d 1002 (9th Cir. 2019) (holding that searches related to gathering evidence of a crime require a warrant). In this case, it is abundantly clear that Agent Bianchi was investigating Didani for a criminal case and this was not an attempt to interdict contraband. For example, that he was "trying to make it so Didani did not miss his connecting flight." Tr. at 41:23-25. The necessary implication is that he was not looking to stop Didani or his luggage, he was trying to investigate Didani. Agent Bianchi testified to investigating Didani, surveilling him and his connections, and otherwise attempting to build a case.

The same is true of the 2016 manual search by SA Nugent, who testified that he was actively looking for "evidence of a crime," *including,* "drug smuggling and drug distribution" because Didani "was under investigation" for both. Tr. at 283-284. That is not an attempt to keep Didani or his luggage out of the country. "The search here was not for digital contraband" and "applying *Cano's* logic would lead to the same result." *Smith,* at *9.

The Court should also be aware that discovery in this case reveals this approach – avoiding the warrant requirement by using the border search exception - is being employed against numerous people just in this case alone. Discovery reveals that Puzio *and his wife* had their phones copied in 2018. There are two other witnesses who the same method was used that Defendant won't place their name in the record at this time. This is a wide-ranging criminal investigation that is unconnected to the narrow border search exception rationale.

At bottom, the reason is self-evident. This is an end run around the Fourth Amendment. It is a subterfuge to build a case without probable cause. To protect the innocent, this Court must act because the conduct here is unrestrained and outrageous.

C. The 2016 Seizure of Didani's Cell Phone Violated CBP Policy

In Didani's Motion to Suppress, the Government's Answer, and Didani's Reply, the parties all agreed that CBP policies applied to the conduct at the border in this case. *See* Gov't Answer at ECF No. 65, PageID.473-475. But the parties disagreed about whether the policy was followed, and even if it was not, whether Didani is entitled to a remedy. *See,*

generally, ECF No. 53, 65, and 70. The issue was never whether the CBP policies applied.

In fact, the government stipulated at the hearing that it produced in discovery two CBP policies. Tr. at 169:3-5; 169:7-16. These policies were entered into evidence as Defendant's Exhibit 2 and 3. Further evidence, of course, that the Government, presumably via law enforcement, agreed that CBP policy applied. Agent Bianchi testified that he was "a part of [the] discovery process." Tr. at 167:10. He testified that discovery is a collaborative effort. *Id.* at 165:19; 166:3, 166:6.

It would make sense, then, why the Government produced CBP policies in discovery. Agent Bianchi, a part of the United States Border Patrol, a division of CBP, would produce CBP policies when asked. It was curious to counsel on Saturday, April 22, 2023, two days before the evidentiary hearing, that the Government e-mailed an ICE (HSI) policy related to border searches. It was curious because of the late hour, and even more curious when Agent Bianchi had no idea what the HSI policy was. Tr. at 166:14-17 (Asked what HSI rule he was referring to, Agent Bianchi answered, "I do not [know]"); 166:18-19 (when asked what it said, Agent Bianchi answered, "I do not [know]").

Thus, before the Court even engages in an analysis of which policy *should* apply, the Court should consider precluding the argument that the HSI policy applies. The fact that the Government produced the CBP policies, not the HSI policy, the fact that Agent Bianchi works for USBP (Tr. at 120:21-23, "Your checks are signed by the United States Border Patrol . . .[Answer:] Correct"), USBP comes under CBP (*see infra,* CBP Policy ¶2.2), and the government argued that CBP policies controlled, it should be precluded from now arguing it did not apply. Because that is clearly what law enforcement and the DOJ thought applied when this conduct occurred.

Nevertheless, even on the merits, the CBP policy should apply. The relevant CBP policies provided by the government and relied upon in prior briefing has the following pertinent provisions:

> 2.1 CBP will protect the rights of individuals against unreasonable search and seizure and ensure privacy protections while accomplishing its enforcement mission.
>
> 2.2 All CBP Officers, Border Patrol Agents, Air and Marine Agents, Office of Professional Responsibility Agents, and other officials authorized by CBP to perform border searches shall adhere to the policy described in this Directive and any implementing policy memoranda or musters.
>
> ………………………………………………………

2.7 This Directive applies to searches performed by or at the request of CBP. With respect to searches performed by [ICE], [HSI] Special Agents exercise currently-held border search authority that is covered by ICE's own policy and procedures. When CBP detains, seizes, or retains electronic devices, or copies of information therefrom, and conveys such to ICE for analysis, investigation, and disposition (with appropriate documentation), the conveyance to ICE is not limited by the terms of this Directive, and ICE policy will apply upon receipt by ICE.

5.1.2 Border searches of electronic devices may include searches of the information stored on the device when it is presented for inspection…

5.1.3 Any border search of an electronic device that is not an advanced search . . . may be referred to as a basic search. In the course of a basic search, with or without suspicion, an Officer may examine an electronic device and may review and analyze information encountered at the border…

5.4.1 An Officer may detain electronic devices . . .Unless extenuating circumstances exist, the detention of devices ordinarily should not exceed five (5) days…

5.4.1.1 Supervisory approval is required for detaining electronic devices [] for continuation of a border search after an individual's departure from the port...Port Director; Patrol Agent in Charge; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or other equivalent level manager approval is required to extend any such detention beyond give (5) days.

See Defendant's Exhibit 2, Section 4 and 5. Under these policies, it is clear law enforcement violated their terms, as the cell phones seized in the 2016 search were kept for 11 days before a warrant was sought and no proof of supervisor approval. The Government's initial argument is Agent Bianchi *could* have gotten more time if he wanted and that courts generally should not suppress evidence for failure to comply with procedure rules.

But the Government has a new position now at the eleventh hour. It is saved, it thinks. An HSI policy produced at the evidentiary hearing, and to counsel two days prior to the hearing, months after the completion of briefing, provides for the following: "Searches are generally to be completed within 30 calendar days of the date of detention…" *See* ¶ 8.1 of HSI Policy.[14]

As a threshold matter, the Court needs to determine which policy should apply, and then consider whether the policy was violated and whether that should lead to suppression. The latter issues have been briefed. *See* parties arguments at ECF No. 53, 65, and 70 regarding CBP policies application and remedies.

[14] It is unclear from the transcript which hearing exhibit is the HSI policy.

The question here is whether the CBP policy or HSI policy should apply to the detention of the cell phone in 2015. The answer is the CBP policy for several reasons.

First, the fact that the Government produced the CBP policy should give this Court great caution in affording any credibility to their position that any of its witnesses *actually* relied on the HSI policies. Indeed, the CBP policy provides that it governs not only CBP officers, but also "Border Patrol" agents, for which Agent Bianchi is one. *See* ¶2.1, CBP Policy, Defendant's Exhibit 2; *see also* Agent Bianchi testimony at Tr. at 7:23; 120:23. The likelihood, on a preponderance standard, of what policy the agents on the ground *thought* they were to follow should be relevant in an analysis of whether they violated it. Officer Parisi was clear that he believed he was operating under CBP policy when he acted. Tr. at 248:19-22.

Second, HSI commissioned CBP to carry out its search and seizure. CBP Officer Parisi acknowledged that often times many federal agencies have to rely on CBP to conduct interviews and searches on the other agencies' behalf. *Id.* at 227:16-17. That is because CBP works "hand in hand together" with these other agencies, including HSI. *Id.* In fact, because "that airport that's kind of [CPB's] house…[CPB] expect[s] a courtesy to either let

[CPB] know, and we'll do the inspection." *Id.* at 227:21-23. Officer Parisi said they have to follow policy and procedure and they expect to decide the course of action. *Id.* at 228. Specifically:

> [Defense counsel]: And you would expect, and correct me if I'm wrong, you would expect that these other agencies would be mindful of your policies and procedures and how CBP handles things; right?
>
> [Officer Parisi]: Yes.

Id. at 228:11-14.

There were no HSI officers present for the interview with Didani on August 6, 2016 – it was two CBP officers. Tr. at 206:19; 211:8; 232:24; 238:20-21 ("it would have only been me and [CBP Officer] Leeker with the subject at that time"). The fact that CBP was commissioned by HSI to handle the search and seizure, and, in fact, CBP did seize the phones and conduct the initial search, is consistent with the plain language of the rule requiring that CBP policies be followed. *See* CBP Policy, Defendant's Exhibit 2, at ¶2.7 ("This Directive applies to searches performed by or at the request of CBP."). The phones were in the custody of CPB when seized. Tr. at 248:6-9.

Third, it is true that CBP policy does provide that "[HSI] Special Agents exercise currently-held border search authority that is covered by ICE's own policy and procedures" and "[w]hen CBP detains, seizes, or

retains electronic devices, or copies of information therefrom, and conveys such to ICE for analysis, investigation, and disposition (with appropriate documentation), the conveyance to ICE is not limited by the terms of this Directive, and ICE policy will apply upon receipt by ICE." But this has to be read in conjunction with the entire policy and in conjunction with the testimony at the hearing.

For example, it would be a perverse incentive to allow one agency to violate its own policy just to be saved by another agency's policy. That could occur here. Had CBP stored the phone for 6 days without further approval, but under the Government's reading, as long as it is handed off to HSI, the violation is meaningless. In order for the rule to make sense, and policy transferring to HSI, this would have had to have been made clear at the hearing that everyone was operating under the belief that HSI policy applied. And that's not the case. All reasonable inferences, as described above, including the disclosure of CBP policy, not HSI, suggests the belief that CBP policy applied.

Accordingly, the only reasonable view of the evidence is that all law enforcement was operating under CBP policy – Agent Bianchi, a member of CBP and, Parisi, a member of CBP.

D. Fruits, Suppression, and Lack of Good Faith.

i. Fruit of the Poisonous Tree and Suppression

Evidence unlawfully seized after a Fourth Amendment violation at the border is subject to a fruit-of-the-poisonous tree analysis and suppression. *See Herring v. United States,* 555 U.S. 135, 141 (2009); *United States v. Laynes,* 481 F. Supp. 3d 657, 668 (SD OH 2020); *see also, e.g., United States v. Rivas*, 157 F.3d 364, 368 (5th Cir. 1998) (suppressing the fruits of an unlawful border search).

The evidentiary hearing made clear that the 2015 search was the critical domino to the entire case. *See, e.g.,* Tr. at 91:13 (Agent Bianchi asked why his investigation changed to its current status: "That would be his cellphone" from 2015); Tr. at 92:13 (Agent Bianchi saw "photos of steroids," later seized in 2016); Tr. at 93:20 (Agent Bianchi saw "multiple cars, high-end cars, and also titles of other people that are not in"). It would be hard to see how the Government could disagree on the importance of the 2015 search: "the images of firearms and bulk, banded currency along with evidence of the movement of money initially found on Didani's iPhone in 2015, single-handedly satisfy the reasonable suspicion threshold." *See* Gov't Answer at ECF No. 65, PageID.465. The unlawful nature of the 2015 search should

render everything that came after, including the 2016 search and seizure should be suppressed.

However, if the Court is unprepared to rule on the suppression at this time, Didani is asking the Court to first identify the constitutional violations that occurred, if any, and then for the parties to determine the extent of the fruits.

ii. Lack of Good Faith

The Court has enough on this record to find a lack of good faith. Agent Bianchi's answers on cross-examination about his decision to forgo a warrant in 2015, for 11 days in 2016, and suddenly apply for one thereafter is enough to show that Agent Bianchi was not acting on some principled basis. *See* Tr. at 150-170. Agent Bianchi strained credulity in trying to explain his decision-making process. He testified he did not apply for a warrant in 2015 because "the evidence that was on the phone that showed criminal activity." *Id.* at 154:14-15. Agent Bianchi then switched his answer: "we were going to search the phone no matter what. It would have been searched whether we had a search warrant or not." *Id.* at 157:8-10. It would have been searched no matter what. In no way does that give the Court a basis to conclude that Agent Bianchi acted "with an objectively reasonable good-

faith belief that [his] conduct [was] lawful." *United States v. Zodhiates,* 901 F.3d 137, 143 (2d Cir. 2018).

The good faith exception should save unlawfully obtained evidence in "circumstances [where] the benefits of police deterrence outweigh the heavy costs of excluding 'inherently trustworthy tangible evidence' from the jury's consideration." *United States v. White*, 874 F.3d 490, 496 (6th Cir. 2017) (quoting *United States v. Leon*, 468 U.S. 897, 907, 104 S. Ct. 3405, 82 L. Ed. 2d 677 (1984)). Given the foregoing discussion about the use of the border exception in such a perverse way, the benefits of deterrence here are *substantial* and outweigh costs of harming a singular drug case in this District.

In *Smith,* Judge Rakoff found that the ultimate obtaining of a warrant saved the evidence obtained from copied cell phones at the border. *Smith, supra,* at *12-13. First, with regard to the 2015 search, the government could not have relied on a warrant that was never issued because it was never sought, nor would it have ever been given on the level of suspicion available at the time. *See Leon,* at 913-918. Second, unlike in *Smith,* "much of the Government's actual search of the copy . . . occurred after a search warrant was issued." *Smith,* at *13. That is not the case here. Agent Bianchi searched

the cell phone in 2015 for a year without a warrant, and 11 days prior to getting a warrant in 2016.

However, if the Court is not inclined to find a lack of good faith, before it analyzes the issue and determines it either way, like the suppression analysis, Didani suggests a decision be made on what, if any, constitutional violations occurred and then the issue of good faith can be address more precisely and perhaps with use of the warrants.

III. CONCLUSION

Didani requests that this Honorable Court enter an order suppressing the evidence obtained from Defendant's cell phones.

Date: July 3, 2023

Respectfully Submitted,

WADE FINK LAW P.C.
/s/ Wade G. Fink
Wade G. Fink (P78751)
Attorneys for Defendant
550 W. Merrill St., Ste 100
Birmingham, MI 48009
wade@wadefinklaw.com

CERTIFICATE OF SERVICE

On July 3, 2023, the foregoing was filed using the Court's e-filing system, which will send notice of same to all parties of record.

/s/ Wade G. Fink

EXHIBIT A

Neutral
As of: July 1, 2023 10:39 PM Z

United States v. Smith

United States District Court for the Southern District of New York

May 11, 2023, Decided; May 11, 2023, Filed

22-cr-352 (JSR)

Reporter
2023 U.S. Dist. LEXIS 82455 *; __ F.Supp.3d __

UNITED STATES OF AMERICA, -v- JATIEK SMITH, ET AL., Defendants.

Prior History: *United States v. Smith, 2023 U.S. Dist. LEXIS 41625, 2023 WL 2446202 (S.D.N.Y., Mar. 10, 2023)*

Core Terms

phone, cell phone, border, searches, border search, digital, wiretap, contraband, governmental interest, traveler's, warrantless search, good faith, copies, seized, probable cause, privacy, stored, suppress, arrest, law enforcement, forensic, objectively reasonable, communications, records, privacy interest, interdicting, interviews, contents, reasons, courts

Counsel: **[*1]** For Sequan Jackson, also known as, Sealed Defendant 2, Defendant: Anthony Cecutti, LEAD ATTORNEY, Law Office of Anthony Cecutti, New York, NY.

For Anthony McGee, also known as, Sealed Defendant 3, Defendant: Jean Desales Barrett, LEAD ATTORNEY, Ruhnke & Barrett, Montclair, NJ.

For Kaheen Small, also known as, Sealed Defendant 4, Defendant: Lisa Scolari, LEAD ATTORNEY, Law Office of Lisa Scolari, New York, NY.

For Damon Dore, also known as, Sealed Defendant 5, Defendant: Michael David Bradley, LEAD ATTORNEY, Bradley Law Firm PC, New York, NY.

For Hasim Smith, also known as, Sealed Defendant 6, Defendant: David Keith Bertan, LEAD ATTORNEY, David K. Bertan, ESQ., New York, NY.

For Rahmiek Lacewell, also known as, Sealed Defendant 7, Defendant: Stephen Turano, LEAD ATTORNEY, Law Offices of Stephen Turano, New York, NY.

For Manuel Pereira, also known as, Sealed Defendant 8, Defendant: Thomas Ambrosio, LEAD ATTORNEY, Thomas Ambrosio, Esq., Lyndhurst, NJ.

For Octavio Peralta, also known as, Sealed Defendant 9, Defendant: Gary Adam Farrell, New York, NY.

For USA, Plaintiff: Rushmi Bhaskaran, LEAD ATTORNEY, United States Attorney's Office, SDNY, New York, NY.

Judges: JED S. RAKOFF, United States District Judge. **[*2]**

Opinion by: JED S. RAKOFF

Opinion

OPINION AND ORDER

JED S. RAKOFF, U.S.D.J.:

By "bottom line" Order dated 3/17/23, the Court denied certain pretrial motions filed by several defendants in this case. See Order, Dkt. 183. This Opinion and Order reaffirms those rulings and sets forth the reasons therefor.

The most significant motion was the motion to suppress evidence filed by defendant Jatiek Smith. By way of background, on March 2, 2021, agents of the federal bureau of Customs and Border Protection ("CBP")[1] detained defendant Jatiek Smith as he returned to Newark airport from Jamaica and forced him to turn over his cellphone and its password. They reviewed the phone manually and created and saved an electronic

[1] All capitalized terms here used refer to the definitions set forth in this Opinion and Order, unless otherwise specified. Also, unless otherwise noted, all internal quotation marks, alterations, omissions, emphases, and citations have been omitted from all cited sources.

copy of it as it existed as of that date and time -- all without a search warrant. Weeks later (after they had already begun reviewing the electronic copy), the Government applied for and obtained a search warrant.

Smith argues, first, that this search violated his *Fourth Amendment* rights. To this much of his motion, the Court agrees. While ***border*** agents have very substantial latitude to search a person's body and effects without a warrant or probable cause during a ***border*** crossing, the Supreme Court has now made clear **[*3]** that ***searching*** the data contained on a person's cell phone is not like ***searching*** his body or pockets. Rather, ***searching*** a cell phone will often allow law enforcement to learn all there is to know about its owner's past movements, communications, and transactions -- reams of information that differ quantitatively and qualitatively from the sorts of information a person could ever have carried with him before the advent of modern "smart" phones. See *Riley v. California, 573 U.S. 373, 134 S. Ct. 2473, 189 L. Ed. 2d 430 (2014)*. Moreover, the vast majority of such information will likely have no connection to the traveler's reasons for crossing the ***border*** on a given day. Furthermore, unlike a traveler's luggage or cargo -- which, quite obviously, is not yet in the country at the time the traveler presents herself for inspection at the ***border*** and can therefore be stopped from coming in -- the information on that traveler's phone most likely already exists *outside* the phone (in cloud storage or other backups), such that a border ***search*** is far less likely to actually prevent anything unwanted from entering or leaving the country.

For these reasons, copying and ***searching*** a traveler's phone during a border crossing bears little resemblance to traditional physical border **[*4]** ***searches*** historically permitted without probable cause under the *Fourth Amendment's* "border search exception." Rather, such searches extend the Government's reach far beyond the person and luggage of the border-crosser -- as if the fact of a border crossing somehow entitled the Government to search that traveler's home, car, and office. The border search exception does not extend so far.

Nonetheless, that still leaves the question whether to suppress the evidence from such an unlawful search. Here, the Court determines that the "good faith" exception precludes suppression, both because at the time of the search, the agents conducting the search had an objectively reasonable basis for believing that there was legal authority binding on them that authorized such a search and also because the Government ultimately obtained a search warrant to search the phone copy, disclosing all relevant details of the search to a neutral magistrate. For these reasons, further elaborated below, the Court reaffirms its prior denial of Smith's motion to suppress.

I. Factual Background

Smith sought to travel from Newark airport to Jamaica on March 2, 2021, where he was denied entry and sent back to the Newark the same day. **[*5]** Gov't Opp. Ex. A, Affidavit of Special Agent Clark ("Clark Decl.") ¶ 14; Declaration of Jatiek Smith ("Smith Decl.") ¶ 3, Dkt. 160. Homeland Security Investigations ("HSI") agents, along with agents of the Federal Bureau of Investigations ("FBI"), were at this time investigating Smith for his and others' alleged role in a putative conspiracy to control the New York area emergency mitigation services ("EMS") industry[2] through an EMS company called "First Response". Clark Decl. ¶¶ 7-8; see also Indictment ¶¶ 2-10, Dkt. 2. Without seeking a warrant, HSI and FBI agents requested CPB agents to search Smith upon his return to Newark Airport "pursuant to [their] border search authority." Clark Decl. ¶ 14. There, border agents searched Smith's bag (in which Smith was carrying just under $10,000 in cash), seized Smith's phone, and demanded his password. Id. Smith claims he repeatedly refused to give his password, relenting only after he was told that "[i]f [he] did not open the phone [he] could be held without charge for as long as it took to open the phone." Smith Decl. ¶ 4. The Government more cryptically represents that "Special Agents . . . requested Smith's passcode, which Smith eventually **[*6]** provided."[3] Clark Decl. ¶ 14.

---

[2] The "EMS industry" refers to companies that provide clean-up services following fires and often also play a role in referring "adjusters" who process fire-related insurance claims. Indictment ¶¶ 1-4.

[3] Smith has not argued that the Government, in holding him at the airport until he turned over his phone password, subjected him to a custodial interrogation under *Miranda v. Arizona, 384 U.S. 436, 86 S. Ct. 1602, 16 L. Ed. 2d 694 (1966)*. Even if Smith had made a *Miranda* argument, however, the Court concludes it would not have mattered. Assuming Smith's interrogation was custodial -- something the Court cannot easily determine on this limited record -- *Miranda* does not require the exclusion of physical evidence obtained based on a suspect's unwarned but voluntary statements. See *United States v. Patane, 542 U.S. 630, 637-42, 124 S. Ct. 2620, 159*

After receiving Smith's passcode, HSI agents made a forensic copy of the phone and returned the original to Smith. Id. In subsequent days, HSI agents began to review the digital copy -- finding, for instance, "communications in which the user of the phone identifies himself as a member of the Bloods and discusses Bloods gang activity," as well as "discussions of Smith's work with First Response, including communications in which he discusses his remuneration arrangement and the 'rules' about responding to fires, as well as communications with what appeared to be either insureds or public adjusters about submitting fraudulent insurance claims." Id. ¶ 15. They also turned over the digital copy to a different group of HSI agents who, in partnership with the FBI, also began reviewing it. Gov't Opp. at 3, Dkt. 168.

Thirty-eight days later (well into multiple law enforcement agencies' review of the digital copy), the Government applied for a warrant to search the forensic copy. See generally Clark Decl.; Gov't Opp. at 3-4. The declaration supporting its application described the airport **[*7]** border search, including that the phone was seized without a warrant "pursuant to HSI's border search authority," and that HSI agents copied the phone's contents and had already begun actively reviewing them. Clark Decl. ¶ 14-15. The declaration also relied in part on evidence from this review -- describing, for example, Smith's communications discussing 'rules' imposed on other EMS companies or the submission of false insurance claims. Id. The declaration also included other evidence that might support a search of the phone, such as witness descriptions of a person named "Teak" (whose description corresponded to Mr. Jatiek Smith's) taking over an EMS company named First Response and proceeding to use violence to set up a "rotation" system through which job assignment in the EMS industry would be shared between companies. Id. ¶ 10. Based on this declaration, Magistrate Judge Aaron issued a search warrant. Clark Decl. at 10 (USAO-000332). The Government's review of the digital copy of Smith's phone continued following the issuance of that warrant. Gov't Opp. at 5.

Six months later, the Government applied for a Title III wiretap on Smith's phone (the same one that had been copied at the **[*8]** border and later searched pursuant to Magistrate Judge Aaron's warrant), as well as the phone of Smith's co-defendant Sequan Jackson. The affidavit in support of the wiretap included evidence from the search of Smith's cellphone, such as excerpts from a WhatsApp conversation between Smith and several of his co-defendants explicitly discussing the "rules" imposed on the industry and the need to discipline other EMS companies that did not follow the "rules". Jackson Ex. A, Clark Affidavit in Support of Wiretap Application ("Clark Wiretap App.") at 15-19. It also included "extensive information provided by witnesses, including accounts from four victims who had been assaulted and/or extorted by First Response," "toll analyses showing that the conspirators communicated with each other, and with victims, by using cell phones," "information from a confidential source," "results from a warrant on Smith's Facebook account, which showed that Smith was publicly advertising his membership in the Bloods gang," and "analyses of financial records, which showed how some of the defendants were paid (either directly or to related corporations) by First Response." Gov't Opp. at 5; Gov't Ex. B at 20-24, **[*9]** 38-42, 47-48, 51-52. Judge Liman, sitting in Part I, authorized the wiretap of Smith's cellphone as well as of his co-defendant Sequan Jackson, which was then extended for one month following a second application and affidavit detailing, among other things, results from the wiretap so far. Gov't Opp. at 5-6; Gov't Ex. C.

II. Smith's Motion to Suppress

Smith moved to suppress both the phone search and the wiretap, on the grounds that they resulted from the border search. That search, Smith contended, violated his *Fourth Amendment* rights.

L. Ed. 2d 667 (2004) (plurality opinion); *id. at 644-45* (Kennedy, J., concurring in the judgment). Further still, even if one assumes that Smith's divulging his password was not just unwarned but also coerced, that would still likely not require suppression. Although courts and commentators have taken varying views on the matter, see Orin Kerr, Compelled Decryption and the Privilege against Self-Incrimination, *97 Tex. L. Rev. 767 (2019)*, the Court holds the view that being made to produce a phone password -- at least, where, as here, there is no real dispute that the person in fact owns the phone and knows its password -- does not violate the *Fifth Amendment's* guarantee against self-incriminating testimony. Id. This is because the *Fifth Amendment* does not prevent compelled production of previously created incriminating evidence where the act of production does not itself involve any incriminating testimony, or where any implicit testimony included in such act of production -- such as acknowledgement of ownership -- can be proved independently. *Fisher v. United States, 425 U.S. 391, 411, 96 S. Ct. 1569, 48 L. Ed. 2d 39 (1976)*.

A. Probable Cause Was Required to Search Smith's Phone

The *Fourth Amendment* provides: "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *U.S. Const. amdt. IV*. As its text makes clear, the "ultimate touchstone . . . is reasonableness[.]" *Brigham City v. Stuart, 547 U.S. 398, 403, 126 S. Ct. 1943, 164 L. Ed. 2d 650 (2006)*. "[W]here a search is undertaken by law enforcement to discover evidence of criminal wrongdoing . . . reasonableness generally requires the obtaining of a judicial warrant." *Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 653, 115 S. Ct. 2386, 132 L. Ed. 2d 564 (1995)*. This "ensures **[*10]** that the inferences to support a search are drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime." ***Riley** v. California, 573 U.S. 373, 382, 134 S. Ct. 2473, 189 L. Ed. 2d 430 (2014)*. "In the absence of a warrant, a ***search*** is reasonable only if it falls within a specific exception to the warrant requirement." Id.

Smith argues that the warrantless ***search*** of his cell phone at Newark airport violated his *Fourth Amendment* rights. To evaluate this argument, this Court must weigh two different strands of precedent: one that gives the Government exceptionally broad authority to effect warrantless searches or seizures at the ***border*** (usually without any kind of heightened suspicion), see II.B.1, infra, and a newer line of cases concerning one's *Fourth Amendment* rights applicable to the vast quantities of sensitive data stored on electronic devices such as cell phones, see II.B.2, infra. The Court summarizes each line of cases, before analyzing how they interact here. See I.B.3, infra.[4]

1) The Border Search Exception

One "exception" to the ordinary requirement that the Government first obtain a warrant before conducting a search relates to border searches. Such searches, "pursuant to the long-standing right of the **[*11]** sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border . . . ." *United States v. Ramsey, 431 U.S. 606, 616, 97 S. Ct. 1972, 52 L. Ed. 2d 617 (1977)*. Citing a customs statute passed by the First Congress that granted customs inspectors the "full power and authority" to search "any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed," *id. at 616* (quoting the *Act of July 31, 1789, c. 5, 1 Stat. 29*), the *Ramsey* Court reasoned that "[b]order searches, then, from before the adoption of the *Fourth Amendment*, have been considered to be 'reasonable' by the single fact that the person or item in question had entered into our country from outside." *Id. at 619*. "The border-search exception is grounded in the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country." *Id. at 620*.

The border-search exception is not, however, entirely unlimited. For instance, the Supreme Court has applied the "reasonable suspicion" standard to the question of whether the Government may detain someone at the border suspected to be "smuggling contraband in her alimentary canal" for long enough for that contraband **[*12]** to be passed. *United States v. Montoya de Hernandez, 473 U.S. 531, 541, 105 S. Ct. 3304, 87 L. Ed. 2d 381 (1985)*. Further, in this and several other circuits, reasonable suspicion is required before the Government may conduct "more personally offensive searches" such as strip searches. *United States v. Asbury, 586 F.2d 973, 976 (2d Cir. 1978)*.

Importantly, these cases make clear that the ***border*** is not a totally *Fourth Amendment*-free zone. Rather, even at the ***border***, "[t]he *Fourth Amendment* commands that ***searches*** and seizures be reasonable," and "[t]he permissibility of a particular law enforcement practice is judged by balancing its intrusion on the individual's *Fourth Amendment* interests against its promotion of legitimate governmental interests." *Montoya, 473 U.S. at 537*. What differs at the ***border*** is the standard of reasonableness, which plays out in a "qualitatively different" way "at the international ***border*** [versus] the

[4] Smith also argues that the border search exception is not even implicated because, since he was denied entry to Jamaica, he did not actually cross any border. Smith Mem. 9, Dkt. 161. The Court disagrees. The fact that Smith was denied entry to Jamaica does not change the fact that the search occurred after Smith had just arrived on a plane from Jamaica and was seeking to reenter the United States. Whether Smith was admitted to Jamaica does not change the fact that he plainly left the United States, such that his return involved a border crossing.

interior." *Id. at 538*.

2) Cell Phones and *Riley* v. California

Neither the Second Circuit nor the Supreme Court has addressed how, if at all, the ***border search*** exception applies to the content of a person's digital cell phone.[5] However, the Supreme Court has provided guidance as to how to think about the problem. Specifically, ***Riley*** *v. California, 573 U.S. 373, 134 S. Ct. 2473, 189 L. Ed. 2d 430 (2014)*, in considering the warrant exception allowing warrantless ***searches*** pursuant to a lawful arrest, the Supreme Court did not automatically extend the exception to ***searches*** of **[*13]** cell phones' digital data. It instead analyzed whether the logic behind the warrant exception applied to cell phone searches. Id. In so doing, the Court made clear its awareness that modern cell phones are materially different from the other types of objects a person might carry because they contain huge quantities of often highly personal data that could not previously have been contained in a pocketable object. *Id. at 393*.

Specifically, to determine whether the rationale for the search-incident-to-arrest exception in fact applied to cell phone searches, the Supreme Court "assess[ed], on the one hand, the degree to which [the search] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Id. at 385* (quoting *Wyoming v. Houghton, 526 U.S. 295, 300, 119 S. Ct. 1297, 143 L. Ed. 2d 408 (1999)*). This "balancing of interests" (which forms the basis for the search-incident-to-arrest exception itself, *id. at 386*[6]) allows warrantless searches of an arrestee's person and pockets so as to ensure officer safety, prevent escape, and safeguard evidence in light of the arrestee's "reduced privacy interests upon being taken into police custody." *Id. at 391*. However, this same balancing had long meant that the exception did not **[*14]** permit warrantless searches of the arrestee's house, which did not implicate the same state interests and would represent "a substantial invasion [of privacy] beyond the arrest itself . . . ." *Id. at 392* (citing *Chimel v. California, 395 U.S. 752, 766-67, 89 S. Ct. 2034, 23 L. Ed. 2d 685 (1969)*).

So too with cell phones. The Court in Riley held that the arresting officer's interest in searching an arrestee to remove dangerous items did not apply to cell phones because "[d]igital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape." *Id. at 387*. Similarly, the government's interest in preventing the destruction of evidence did not support allowing warrantless cell phone searches because, instead, law enforcement could prevent any destruction of digital evidence by turning off the phone, disconnecting it from networks, or placing it in a device meant to secure it from remote wiping until a warrant could be obtained. *Id. at 390-91*. Further, and perhaps most crucially, an individual's privacy interest in his cell phone differed fundamentally from that same individual's privacy interests with respect to his person or the contents of his bags or pockets. *Id. at 393*. This was because "[m]odern cell phones, as a category, implicate **[*15]** privacy concerns far beyond those implicated by the search of" the other sorts of physical items a person might carry in her pocket. Id. Indeed, the Court treated with near scorn the Government's argument "that a search of all data stored on a cell phone is 'materially indistinguishable' from searches of these sorts of physical items," calling that argument "like saying a ride on horseback is materially indistinguishable from a flight to the moon." Id. Instead, the Court made clear that "[a] conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom." Id.

Such an extension, the Court held, failed because the data contained on an arrestee's phone "differ[s] in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person." *Id. at 393*. While "[m]ost people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read[,] nor would they have any reason **[*16]** to attempt to do so . . . the possible intrusion on privacy

---

[5] By "cell phone," the Court means the digital "smartphones" owned by 85% of U.S. adults. Pew Research Center, Mobile Fact Sheet, https://www.pewresearch.org/internet/fact-sheet/mobile/. That such devices act as conventional telephones is almost incidental. They are pocket-size computers that many adults (and non-adults) carry with them at all times and through which they send texts and emails, buy products, navigate to and from destinations, watch entertainment, consume news, participate in social media, search the Internet, take and post photographs and videos, and -- occasionally -- make phone calls.

[6] The same "balancing of interests" underlies the border search exception. See II.B.1, supra; *Montoya, 473 U.S. at 537-38*.

is not physically limited in the same way when it comes to cell phones." *Id. at 393-94*. Further, "a cell phone collects in one place many distinct types of information -- an address, a note, a prescription, a bank statement, a video -- that reveal much more in combination than any isolated record." *Id. at 394*. And cell phones' enormous storage capacity "allows even just one type of information to convey far more than previously possible," such that "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet." Id. Moreover, "the data on a phone can date back to the purchase of the phone, or even earlier," including records of calls and written communications dating back months or years that almost certainly would never be contained in non-digital papers found on a person. Id. And "[f]inally, there is an element of pervasiveness that characterizes cell phones but not physical records." While "[p]rior to the digital age, people did not typically carry a cache of sensitive personal information **[*17]** with them as they went about their day," it is now "the person who is not carrying a cell phone, with all that it contains, who is the exception." Id.

Further still, the kinds of data stored on a cell phone makes them "qualitatively different" from the sorts of physical records or objects a person might carry with them. Id. A person's "Internet search and browsing history" might "reveal an individual's private interests or concerns," such as private medical details. *Id. at 395-96*. Also, "[h]istoric location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." *Id. at 396*. These were just some of the many kinds of highly private data many or most users might have stored on their phone. Id.

Lest there be any doubt, the Court in ***Riley*** noted that while it had previously echoed Judge Learned Hand's 1926 observation "that it is 'a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him' . . . [i]f his pockets contain a cellphone, however that is no longer true." Id. Instead, a "cell phone **[*18]** ***search*** would typically expose to the government far more than the most exhaustive ***search*** of a house: [a] phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form -- unless the phone is." *Id. at 396-97*.

3) Cell Phones at the *Border*

Although ***Riley*** itself concerned ***searches*** incident to lawful arrests, its logic would seem to apply to cell phone ***searches*** at the ***border***. Specifically, as in ***Riley***, a court should decide "whether to exempt a given type of ***search*** from the warrant requirement 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'"[7] *Id. at 385*. In conducting this analysis, courts should not automatically presume that a balance previously struck as to a certain kind of physical search automatically extends to a search of the data contained on a person's cell phone. *Id. at 393*. Rather, courts should independently evaluate whether the governmental interests thought to support a warrant exception actually apply to cell phone searches, and whether the **[*19]** intrusion on privacy posed by a physical ***search*** is relevantly comparable to that posed

---

[7] Riley did include a potential caveat to any need for such a balancing inquiry: specifically, where there is "precise guidance from the founding era," such guidance might resolve the need for a warrant. *Id. at 385*. See also *United States v. Jones, 565 U.S. 400, 406-07, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012)* (looking to the original understanding of the *Fourth Amendment* to determine whether the physical trespass involved in placing a GPS device on a person's car constituted a ***search*** or seizure). It is certainly true that courts have grounded the ***border search*** exception in historical understanding. *Ramsey, 431 U.S. at 616* (discussing a customs statute passed by the First Congress as probative of the *Fourth Amendment's* application to ***border searches***). However, as discussed above, ***Riley*** made clear that courts could not simply extend historical acceptance of warrantless ***searches*** of physical items at a particular time or place to phones; rather, the unique qualitative and quantitative differences between the sort of information contained on cell phones and that contained in physical records requires consideration of whether the logic behind a historically grounded exception applies to cell phones. ***Riley***, *573 U.S. at 393-403*. See also Orin Kerr, *Foreword: Accounting for Technological Change*, *36 Harv. J.L. & Pub. Pol'y 403 (2013)* (arguing for "[t]he need for different rules governing digital devices"); Note, *The **Border Search** Muddle*, *132 Harv. L. Rev. 2278, 2287-99 (2019)* (arguing that it remains unclear how the founding generation thought about ***border searches*** as applied to a person's papers, such that applying the ***border search*** exception to the contents of a cellphone necessarily requires legal reasoning beyond historical description).

by a ***search*** of cell phone data. See *id. at 385-403*. See also *United States v. Aigbekaen, 943 F.3d 713, 720 (4th Cir. 2019)* ("[A] warrant exception will not excuse a warrantless ***search*** where applying the exception would untether the rule from the justifications underlying it."). Application of ***Riley*** at least this far should prove uncontroversial, as the Supreme Court has indicated that the ***border search*** exception is itself the product of precisely this kind of balancing of interests. *Montoya, 473 U.S. at 538-39*.

Applying this balancing framework to phone ***searches*** at the ***border*** yields the same result as in ***Riley***. None of the rationales supporting the ***border search*** exception justifies applying it to ***searches*** of digital information contained on a traveler's cell phone, and the magnitude of the privacy invasion caused by such ***searches*** dwarfs that historically posed by ***border searches*** and would allow the Government to extend its ***border search*** authority well beyond the ***border*** itself. As such, the Court concludes that the Government may not copy and ***search*** an American citizen's[8] cell phone at the ***border*** without **[*20]** a warrant absent exigent circumstances.

In reaching this conclusion, the Court first considers, as in ***Riley***, the governmental interests previously relied upon to support the warrant exception urged here. ***Border***-***search*** cases often refer at a fairly general level to the Government's interest in "the protection of the integrity of the ***border***," which of course includes the Government's interests in preventing the introduction into this country of illicit substances or contraband. *Montoya, 473 U.S. at 536-38*. The Government's interests also include apprehending persons who may pose a threat or who lack authorization to be present in this country, *United States v. Martinez-Fuerte, 428 U.S. 543, 556, 96 S. Ct. 3074, 49 L. Ed. 2d 1116 (1976)*, in inspecting goods to ensure appropriate customs tax is paid, *Ramsey, 431 U.S at 616*, and more generally "protecting this Nation from entrants who may bring anything harmful into this country, whether that be communicable diseases, narcotics, or explosives." *Montoya, 473 U.S. at 544*. In other words, the Government has a very strong interest in preventing unwanted persons or items from entering the country.

But despite the strength of this interest, it is hard to see how it applies to searches of the digital data contained on a traveler's cell phone. When the Government interdicts contraband, identifies goods subject **[*21]** to customs tax, or prevents someone from entering the country without authorization, it successfully stops a person or thing outside the country from unlawfully coming into it. But data stored on a cell phone is not like that -- it instead can and very likely does exist not just on the phone device itself, but also on faraway computer servers potentially located within the country. And, wherever the servers are located, the owner of a cell phone can generally access or share part or all of the data on it with anyone else in the world so long as both parties have an internet connection. Stopping the cell phone from entering the country would not, in other words, mean stopping the data contained on it from entering the country. See, e.g., Orin Kerr & Robert Wisberg, *Searching Computers at the Border* (Stanford Law School Zoom Event, 3/3/22), https://www.youtube.com/watch?v=WflaKYW1jUI. See also Jennifer Daskal, *The Un-Territoriality of Data*, *125 Yale L.J. 326, 365-77 (2015)* (discussing the challenges the diffusion of data poses to firm concepts of territoriality).

Some courts have suggested that cell phones might contain so-called "digital contraband" such as explicit images involving the sexual abuse of children. See, **[*22]** e.g., *United States v. Cano, 934 F.3d 1002, 1014 (9th Cir. 2019)* (reasoning that "because cell phones may ultimately be released into the interior . . . the United States has a strong interest in preventing the entry of such material."). Given what the Court has just discussed about how digital data exists separate and apart from the physical cell phone on which it is stored, the Court doubts that the Government's interest in interdicting such "digital contraband" as it exists on a specific device -- when the exact same digital contraband likely is already stored outside the device and available to its owner and others within this country -- is genuinely comparable to the Government's interest in interdicting physical contraband. Physical contraband, once interdicted, will not enter the country, whereas digital contraband easily could and very likely already has. But, in any event, no party seriously contends that the search of Smith's phone in this case was for "digital contraband," so the Court need not definitively resolve the precise extent of the Government's interest in interdicting digital contraband. Cf. *id. at 1019-21*

[8] The Court need not here address whether the same result would hold for a non-resident or non-citizen. Cf. *United States v. Verdugo-Urquidez, 494 U.S. 259, 261, 110 S. Ct. 1056, 108 L. Ed. 2d 222 (1990)* (holding that the *Fourth Amendment* does not protect property held in Mexico by a Mexican resident and citizen against search or seizure by the U.S. Government).

(reasoning that while ***border*** agents could conduct warrantless forensic ***searches*** of phones for digital contraband with reasonable **[*23]** suspicion, they could not conduct warrantless phone ***searches*** for anything other than digital contraband). Therefore, while the Court acknowledges the Government's strong interest in ***searching*** persons or physical objects at the ***border***, any corresponding interest in ***searching*** the digital data "contained" on a particular physical device located at the ***border*** is relatively weak. Kerr & Wisberg, supra at 18:00-20:00.

The Court weighs against this relatively weak governmental interest a citizen's privacy interests in her cell phone data at the time she presents herself at a U.S. ***border***. Just as in ***Riley***, the cell phone likely contains huge quantities of highly sensitive information -- including copies of that person's past communications, records of their physical movements, potential transaction histories, Internet browsing histories, medical details, and more -- that this Court has already addressed at some length. Section II.B.2, supra; ***Riley***, 573 U.S. at 394-97. To be sure, an individual who presents herself at a ***border*** crossing has diminished privacy interests because she should reasonably expect that her person or possessions may be subject to ***search***. Montoya, 473 U.S. at 539-40. Similarly, an individual subject to arrest and impending detention has substantially **[*24]** "reduced privacy interest[s] upon being taken into police custody." ***Riley***, 573 U.S. at 391. But, just as in ***Riley***, this kind of reduced privacy interest has always been understood with respect to the physical things a person carried with her -- whether at the time of the arrest or, as here, at the time of a ***border*** crossing. Technological and cultural changes now mean that nearly all travelers carry with them, in additional to any physical items, a digital record of more information than could likely be found through a thorough ***search*** of that person's home, car, office, mail, and phone, financial and medical records, and more besides. No traveler would reasonably expect to forfeit privacy interests in all this simply by carrying a cell phone when returning home from an international trip. Because the government's interests in a warrantless ***search*** of a cell phone's data are thus much weaker than its interests in warrantless ***searches*** of physical items, and a traveler's privacy interests in her cell phone's data are much stronger than her privacy interests in her baggage, the Court concludes that the same balancing test that yields the ***border*** ***search*** exception cannot support its extension to warrantless cell **[*25]** phone ***searches*** at the ***border***.[9]

In holding that warrants are required for cell phone ***searches*** at the ***border***, the Court believes it is applying in straightforward fashion the logic and analysis of ***Riley*** to the ***border*** context. Importantly, however, the Court recognizes that of the five federal courts of appeals to consider the question, none has gone quite this far (although the Ninth Circuit has come close). But it is clear that both the Ninth Circuit and the Fourth Circuit would have required a warrant for the ***search*** conducted here.

Specifically, the Ninth Circuit held in 2019 that ***border*** officials may conduct warrantless ***searches*** of cell phones "only to determine whether the phone contains contraband," such as explicit images of child sexual abuse. Cano, 934 F.3d at 1018. ***Searches*** for evidence relating to a crime (such as the ***search*** here) require a warrant, because the Government's interest in obtaining evidence -- as opposed to interdicting contraband or other unwanted items or persons -- is not materially different at the ***border*** than elsewhere. Id. at 1016-19.

As there is no dispute that the search here was not for digital contraband, applying Cano's logic would lead to the same result in this case that the Court independently **[*26]** reaches: that the warrantless search and copying of Smith's phone was unlawful. As to Cano's other holding -- that warrantless searches for digital contraband are permissible, whether without any heightened suspicion in the case of "manual" searches (scrolling through someone's phone), or with reasonable suspicion in the case of more thorough "forensic" searches, id. at 1012-16 -- the Court doubts that the Government's interest in interdicting so-called "digital" contraband is genuinely comparable to its historically grounded interest in interdicting physical contraband, since, as discussed above, digital data is rarely stored uniquely on a cell phone such that seizing such a phone with unwanted data really would mean preventing that data from "entering" the country. However, the Court

---

[9] This of course does not mean that under exigent circumstances, the Government could not conduct warrantless phone searches or seizures at the border. Kentucky v. King, 563 U.S. 452, 460, 131 S. Ct. 1849, 179 L. Ed. 2d 865 (2011). The Court need not here address whether circumstances that might not qualify as exigent within the country could qualify in the border context. The Court likewise need not address whether the Government may have relatively greater leeway at the border than elsewhere to temporarily seize or copy a phone until it is able to apply for a warrant.

need not definitively resolve that question, since there is no question that the search here was not for digital contraband.

Applying similar logic to *Cano*, the Fourth Circuit in *United States v. Kolsuz, 890 F.3d 133 (4th Cir. 2018)* likewise reasoned that a warrantless search of a cell phone at the border is impermissible absent some nexus between the Government's interests in protecting the border and the search. *Id. at 143*. However, unlike the Court in *Cano*, the Fourth Circuit reasoned **[*27]** that such a "nexus" could be satisfied not just by the phone containing actual digital contraband but also by its containing evidence of a border related violation (such as, as in *Kolsuz*, suspected smuggling of firearms). Id.

As noted by the *Cano* court, this reasoning effectively enlarges the border search exception, by transforming a warrant-exception based on the Government's interest in preventing the introduction of unwanted persons or things into an interest in "search[ing] for *evidence* of contraband that is *not* present at the border." *Cano, 934 F.3d at 1018*. Of course, whether at the border or elsewhere, the Government has a strong interest in obtaining evidence of illegality, including illegality that may occur at the border. But, just as that interest cannot support the Government's conducting a warrantless search of a person's house simply because it believes it may contain evidence of a crime, it does not support allowing the Government to conduct warrantless searches of cell phones for evidence of border-related crimes. Id. However, notwithstanding this Court's disagreement with the Fourth Circuit's approach, the Court notes that even under that approach, the warrantless phone search conducted here for **[*28]** evidence of crimes having nothing to do with the border would not have been permissible. See *United States v. Aigbekaen, 943 F.3d 713, 720-21 (4th Cir. 2019)* ("[T]he Government may not invoke the border exception on behalf of its generalized interest in law enforcement and combatting crime.").

It is important to note, however, that two other circuit courts to address the question have held that the Government may search cell phones at the ***border*** without a warrant and without any heightened requirement of nexus between the search and the Government's interests in preventing the entry of unwanted persons or items. See *Alasaad v. Mayorkas, 988 F.3d 8, 21 (1st Cir. 2021)*; *United States v. Touset, 890 F.3d 1227, 1235 (11th Cir. 2018)*. Additionally, the Eighth Circuit recently indicated its likely agreement with the First and Eleventh Circuits, although, since the Government's ***search*** in that case sought to uncover evidence of trade secrets being smuggled out of the country, the court declined to definitively resolve whether there is any nexus requirement. *United States v. Xiang, 2023 U.S. App. LEXIS 11027, 2023 WL 3263857, at *4-6 (8th Cir. 2023 May 5, 2023)*. In any event, none of these decisions is persuasive to this Court or binding upon it.

The First Circuit sought to distinguish ***Riley*** by stating that "[t]he ***search*** incident to arrest warrant exception [at issue in ***Riley***] is premised on protecting officers and preventing evidence destruction, rather than on addressing **[*29]** ***border*** crime." *Alasaad, 988 F.3d at 21*. It further emphasized that the "***border search*** exception's purpose is not limited to interdicting contraband; it serves to bar entry to those 'who may bring anything harmful into this country' . . . [including] 'communicable diseases, narcotics, or explosives.'" *Id. at 20*. This Court agrees that the governmental interest underlying the ***border search*** exception is different from that underlying the ***search***-incident-to-arrest exception, and it acknowledges that the former extends to preventing a wide variety of harmful things from entering the country. But, as discussed above, "things" are different from "data", so it is hard to see why the interests underlying the ***border search*** exception extend to the data stored on a traveler's cell phone. To be sure, that data may contain information relevant to the Government's determination as to whether a person should be allowed entry, but the Government has little heightened interest in blocking entry of the information itself, which is the historical basis for the border search exception. The Government's more general investigative interest in data about the person or thing entering the country is entirely incidental to the fact of the **[*30]** cell phone being carried over the border, and could just as easily be relied upon to support searches of the person's home, records, or past mail far away from the border.

The Eleventh Circuit, meanwhile, relied heavily on the example previously discussed of "digital contraband" such as explicit sexual material involving minors (which is not surprising, since the case involved a search for such material). *Touset, 890 F.3d at 1232-33*. Putting aside this Court's previously expressed doubts as to the strength of the Government's interest in preventing the entry of a particular device containing such material -- which, more likely than not, is also stored outside the device and already accessible within this country -- any interest in seizing "digital contraband" would not justify

warrantless searches for other purposes, as the Ninth Circuit made clear in *Cano, 934 F.3d at 1018*. The Eleventh Circuit meanwhile brushed aside the Supreme Court's reasoning in Riley as concerns the unique privacy implications of cell phone searches, arguing that "it does not make sense to say that electronic devices should receive special treatment because so many people now own them or because they can store vast quantities of records or effects" since "[t]he **[*31]** same could be said for a recreational vehicle filled with personal effects or a tractor-trailer loaded with boxes of documents." *Touset, 890 F.3d at 1233*. The analogy seems weak on its face: relatively few travelers cross the border in an RV or truck with all their personal possessions and documents in store, while this Court surmises that most travelers carry a cell phone. More to the point, as the Supreme Court made clear in Riley, the storage capacity and pervasive use of cell phones in every aspect of users' lives make them qualitatively and quantitatively different from the sorts of possessions or records a person might carry with her. ***Riley**, 573 U.S. at 393*. True, the ***Riley*** court made that observation in the context of considering the kinds of objects a person might have on their person or perhaps in their car at the time of an arrest, while it might be likely that travelers at the ***border*** carry relatively more physical objects with them. But the basic point -- that a cell phone carries far more and far more sensitive information than would historically have been contained in carriable physical objects -- plainly applies at the ***border*** as well.

Finally, and quite recently (well after the ***search*** in this case), the Eighth Circuit **[*32]** distinguished ***Riley*** on the barebones basis that it "involved a different *Fourth Amendment* exception, ***searches*** incident to arrest," without explaining why the logic of ***Riley*** does not apply in the ***border*** context. *Xiang, 2023 U.S. App. LEXIS 11027, 2023 WL 3263857, at *3*. As already explained, the Court agrees that ***Riley*** does not extend automatically to the ***border search*** context, but the Court disagrees that this alone serves to distinguish it. Rather, courts should apply the methodology ***Riley*** laid out for evaluating when a warrant exception applies to the data contained on phone ***searches*** by balancing the governmental interests supporting the exception against the privacy interests implicated -- the same exact balancing test used to produce the underlying warrant exceptions, ***Riley**, 573 U.S. at 386*; *Montoya, 473 U.S. at 538-39*. Applying that methodology, it seems clear that the ***border search*** exception should not extend to warrantless ***searches*** of the data contained on cell phones. In any event, the Eighth Circuit did not definitively resolve whether a warrantless ***border search*** of a cell phone requires some nexus to a ***border***-related rationale (as held by the Ninth and Fourth Circuits), since it reasoned that the ***search*** in that case -- for trade secrets the defendant was suspected of smuggling abroad -- plainly **[*33]** had such a nexus. Id.

For the foregoing reasons, the Court concludes that the warrantless ***search*** of Smith's cell phone was unreasonable under the *Fourth Amendment*. As discussed above, this Court's preferred rule --that phone ***searches*** at the border generally require warrants outside exigent circumstances -- is somewhat more protective than the approach of any circuit court to consider the question. But even under the approaches of the Fourth and Ninth Circuits, a warrant would have been required to search Smith's phone since this was neither a search for digital contraband nor for evidence of physical contraband. *Cano, 934 F.3d at 1018*; *Aigbekaen, 943 F.3d at 720-21*. Thus, whether the Government must obtain a warrant for all border cell phone searches (absent exigent circumstances), or just those border phone searches not immediately connected with preventing unwanted persons or things from entering the country, a warrant was required here.

B. Whether to Suppress the Phone Search

Deciding that the border search of Smith's cell phone was unlawful does not, however, answer whether the results of the search should be suppressed. After all, "[e]xclusion is 'not a personal constitutional right,' nor is it designed to 'redress the injury' occasioned by an unconstitutional **[*34]** search," but rather is meant "to deter future *Fourth Amendment* violations." *Davis v. United States, 564 U.S. 229, 236-37, 131 S. Ct. 2419, 180 L. Ed. 2d 285 (2011)*. Accordingly, while courts will ordinarily exclude evidence obtained in violation of the *Fourth Amendment*, such evidence may still come in under various exceptions to the exclusionary rule. The Government argues that three such exceptions -- the independent source, inevitable discovery, and good faith exceptions -- are implicated here. The Court discusses each in turn.

1) The search of Smith's phone did not derive from an independent source

The Government first invokes the "independent source" exception, which allows the Government to rely at trial on evidence obtained in violation of the *Fourth*

Amendment in some circumstances if it can show that it would have obtained the evidence in any event pursuant to a later and lawfully obtained warrant. See *Murray v. United States, 487 U.S. 533, 542, 108 S. Ct. 2529, 101 L. Ed. 2d 472 (1988)*. The Government argues that because Magistrate Judge Aaron ultimately issued a warrant to search the electronic copy of Smith's cell phone during the border search, and the affidavit filed in support of its warrant application included information beyond that already found on Smith's cell phone (such as witness accounts describing Smith's conduct), the ultimate search of Smith's phone was based on probable cause **[*35]** independent of the border search. Gov't Opp. at 17-18; Gov't Sur-Reply at 7, Dkt. 181.

The Court disagrees. For the independent source exception to apply, two conditions must hold. First, "the warrant must be supported by probable cause derived from sources independent of the illegal entry." *United States v. Johnson, 994 F.2d 980, 987 (2d Cir. 1993)*. Second, "the decision to seek the warrant may not be prompted by information gleaned from the illegal conduct." Id. Neither condition is met here.

In this regard, the Court disagrees with the Government's claim that the warrant the Government ultimately obtained was "substantially based on information that was untethered to the cursory" search of the phone already performed at the time it sought the warrant. Gov't Opp. at 17. To be sure, the affidavit submitted in support of the Government's warrant application included significant independent evidence of Smith's potentially unlawful conduct, including the results of witness interviews, information taken from Smith's social media page, and more. However, other than relatively conclusory assertions that evidence of the sort sought generally exists on cell phones, the only specific information indicating that evidence of illegality would likely be **[*36]** found on Smith's phone were descriptions of already-reviewed text messages that indicated Smith's membership in the Bloods gang as well as his role in enforcing "rules" on other emergency mitigation companies as to how to respond to fires. Clark Decl. ¶ 15. As such, the Court seriously doubts that the warrant application stood on its own in establishing probable cause absent the information it contained about the evidence stored on Smith's phone.

More fundamentally, the ultimate search of the forensic copy of Smith's phone could not have been "independent" of the initial unlawful search, because the forensic copy existed only because of that search. Even if the Government had independent probable cause to search Smith's cell phone at the time it obtained its warrant, the search it actually performed was of a copy of Smith's cell phone made during the border search -- a copy that almost certainly contained at least somewhat different data from the actual phone at the later moment when the Government obtained a warrant. Accordingly, the search was plainly not independent of the unlawful border search.

2) The cell phone search was not inevitable.

For similar reasons, the Government cannot **[*37]** rely on the "doctrine of inevitable discovery," which applies when the Government can "establish by a preponderance of the evidence that the information ultimately or inevitably would have been discovered by lawful means." *United States v. Eng, 971 F.2d 854, 859 (2d Cir. 1992)*. Once again, the difficulty is that because the Government searched a copy of Smith's phone made during the initial search, any later search of that forensic copy -- as opposed to a search of the data contained on Smith's phone at a later point in time -- would not probably have occurred but for the initial unlawful search. See, e.g., Orin Kerr, *The Fourth Amendment Limits of Internet Content Preservation*, *65 St. Louis U. L.J. 753, 807 (2021)* ("Applying the inevitable discovery exception leads to a simple outcome . . . [i]f the preservation copy is the fruit of an unconstitutional seizure, then it should not have existed and it cannot be used."). Since the copy of Smith's cell phone containing the data existing as of the date and time of the border search would not have existed but for the unlawful search -- and since the data contained on Smith's actual phone as of the time the warrant issued may have materially differed from the data contained on the copy -- the warranted search of the phone copy was not inevitable. **[*38]**

3) The Good Faith Exception

Finally, the Government argues that the good faith exception to the exclusionary rule applies. That exception allows unlawfully obtained evidence to be used at trial "when the Government acts with an objectively reasonable good-faith belief that their conduct is lawful." *United States v. Zodhiates, 901 F.3d 137, 143 (2d Cir. 2018)*. The Government has therefore been allowed to rely on unlawfully obtained evidence where, for instance, "the police conduct a search in objectively reasonable reliance on a warrant later held invalid," where "searches [are] conducted in reasonable

reliance on subsequently invalidated statutes," or where "the police conduct a search in objectively reasonable reliance on binding judicial precedent." *Davis v. United States, 564 U.S. 229, 239-40, 131 S. Ct. 2419, 180 L. Ed. 2d 285 (2011)*. Generally, exclusion is appropriate "[w]hen the police exhibit 'deliberate,' 'reckless,' or 'grossly negligent' disregard for *Fourth Amendment* rights [because] the deterrent value of exclusion is strong and tends to outweigh the resulting costs." *Id. at 238*. However, "when the police act with an objectively 'reasonable good-faith belief' that their conduct is lawful, or when their conduct involves only simple, 'isolated' negligence, the 'deterrence rationale loses much of its force,' and exclusion cannot 'pay its way.'" **[*39]** *Id. at 238*.

The Government here offers two good faith arguments: first, that the initial border search, even if unlawful, itself falls under the good faith exception, and second, that the Government's later reliance on Magistrate Judge Aaron's warrant falls under the good faith exception. The Court agrees with both arguments.

i) The Government's initial border search falls under the good faith exception.

As to the first argument, the breadth of the "border search exception" was still largely in place at the time of the search. Indeed, two of four federal circuit courts of appeals that had addressed forensic searches of cell phones at the border had held that such seizures and searches were lawful without warrants independent of any nexus between the search and a border-related rationale.[10] While two other circuit courts had indicated to the contrary, given the historic breadth of the "border search exception," a reasonable government agent could have a good faith belief that such a search as was conducted here was permissible absent Supreme Court or Third Circuit precedent to the contrary.

Furthermore, even if that were not enough, a reasonable border agent could have in good faith believed that the **[*40]** search conducted here was expressly warranted by a 2018 CBP directive, which purports to allow so-called "manual" phone searches at the border without any heightened standard of suspicion and "advanced search[es]" -- which entail "connect[ing] external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents" -- whenever "there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP"[11] or "when there is a national security concern. . . ." CBP Directive No. 3340-049A at 4-5, U.S. Customs and Border Protection (Jan. 4, 2018), Dkt. 159-1.

"Reasonable suspicion" is, of course, a modest standard requiring much less than the "probable cause" required for a warrant. The Government contends there was reasonable suspicion here either because of the information its investigation of Smith's domestic activities had already yielded, or because of the circumstances of Smith's arrival at Newark Airport from Jamaica in March 2021, when he had left Newark earlier that day and been denied entry in Jamaica and was carrying just under $10,000 in cash. **[*41]** Gov't Opp. at 15. At the very least, the information later presented to Magistrate Judge Aaron in obtaining a warrant clearly indicates that, even prior to the search, the Government had objectively reasonable suspicion of Smith's involvement in criminal activity. The border agents who searched Smith at the express request of the government agents conducting the underlying investigation thus had more than a good faith basis for believing that they were acting under the authority of the 2018 CBP directive in seizing and searching Smith's cell phone.[12]

This conclusion is further reinforced by the Second Circuit's decision in *United States v. Levy, 803 F.3d 120 (2d Cir. 2015)*, in which it held that a CBP agent could search and copy the contents of a traveler's notebook

---

[10] The most applicable circuit (the Third, because the phone was seized at Newark airport) had not addressed the issue at all.

[11] The Government represents that Title 18 of the U.S. Code is one of almost 30 titles enforced in some capacity by CBP. Gov't Opp. at 13 (citing "Summary of Laws Enforced by CBP," *available at* https://www.cbp.gov/trade/rulings/summary-laws-enforced/us-code).

[12] Of course, law enforcement agencies cannot launder unconstitutional practices by promulgating internal guidance that does not itself demonstrate an objectively reasonable good faith effort to apply the law, as any "good faith" reliance by line officers on such guidance would depend on the bad faith of their superiors. Here, however, the CBP guidance document, which requires reasonable suspicion for forensic searches, was more protective than what some courts had held to be required, *Touset, 890 F.3d at 1233*, and reflects an objectively reasonable attempt to apply the law in this unsettled area.

based on reasonable suspicion of the traveler's involvement in financial crimes that other government law enforcement agencies were investigating. *Id. at 122-24*.[13] There, the Second Circuit rejected the traveler's argument "that border searches conducted by the CBP, even at the prompting of another federal agency, should at least be confined to crimes that a statute or regulation specifically authorizes CBP to investigate," and instead reasoned that "CBP officers are neither expected **[*42]** nor required to ignore tangible or documentary evidence of a federal crime." *Id. at 124*(stating that CBP agents "have the authority to search and review a traveler's documents and other items at the border when they reasonably suspect that the traveler is engaged in criminal activity, even if the crime falls outside the primary scope of their official duties"). While *Levy* is distinguishable from the instant case because it dealt with a physical notebook, rather than a cell phone (which, as discussed extensively above, poses unique privacy concerns, see II.A.2-3, supra), it nonetheless supports the contention that government agents considering the law as it existed at the time of the border search could reasonably believe they had a binding lawful basis for seizing and searching Smith's cell phone.

In short, because the agents who requested the search had objectively reasonable suspicion to so request and the agents who actually conducted the search had what they could have reasonably considered as binding authority to do so under the 2018 CBP Directive, the search meets the requirements for the good faith exception to the exclusionary rule.

ii) The Government properly relied on a later-issued warrant [*43]

Independent of its conclusion that the good faith exception applies to the Government's initial unlawful phone search, the Court separately concludes that the good faith exception precludes suppression of the fruits of that search because the Government ultimately obtained a search warrant. The core good faith exception to the exclusionary rule applies where the Government reasonably relies on a duly issued search warrant, even if that warrant should never have issued. *United States v. Leon, 468 U.S. 897, 913-18, 104 S. Ct. 3405, 82 L. Ed. 2d 677 (1984)*. Here, much (though not all) of the Government's actual search of the copy made of Smith's phone occurred after a search warrant was issued by Magistrate Judge Aaronson. Clark Decl. ¶ 14; Gov't Opp. at 3-4. True, the Government obtained that warrant after the initial search occurred, and in order to establish probable cause, the Government relied in its warrant application on information already obtained (in this Court's view, unlawfully) from Smith's phone. Clark Decl. ¶¶ 14-15. But it disclosed the relevant circumstances of the search -- including that CBP agents seized, copied, and began searching Smith's phone without a warrant at the border in order to further non-border related investigations of other government **[*44]** agencies -- to Magistrate Judge Aaron.

The Second Circuit has previously applied the good faith exception in similar circumstances to these. In *United States v. Thomas, 757 F.2d 1359 (2d Cir. 1985)*, DEA agents used a dog to smell directly outside a suspect's apartment to determine whether drugs were inside. *Id. at 1366*. Based in significant part on the results of this "canine sniff," the Government applied for and obtained a search warrant to search the suspect's home. Id. The Second Circuit agreed with the defendant that the initial canine sniff was itself an unconstitutional search, conducted without a warrant or probable cause. *Id. at 1366-67*. It further agreed that -- without the results of the unconstitutional canine sniff -- there was no probable cause to search the defendant's home, such that no search warrant should have issued. *Id. at 1367-68*. But, notwithstanding that determination, the Second Circuit concluded that suppression would be inappropriate, because the Government "brought [its] evidence, including the positive 'alert' from the canine, to a neutral and detached magistrate," and "[t]hat magistrate determined that probable cause to search existed, and issued a search warrant." *Id. at 1368*. Since "[t]he magistrate, whose duty it is to interpret the law, determined that **[*45]** the canine sniff could form the basis for probable cause[,] it was reasonable for the officer to rely on this determination." Id.

This is not to say a later-issued warrant that relies for probable cause on unconstitutionally obtained information always suffices to establish good faith. Where law enforcement agents fail to disclose relevant facts to the magistrate, or have independent reason to know their actions were unconstitutional, then a later obtained search warrant will not automatically establish good faith. See *United States v. Reilly, 76 F.3d 1271, 1281 (2d Cir. 1996)*. But where "the issuing magistrate

[13] Although the agents who carried out the search at Newark airport were directly subject to Third Circuit law, they were acting at the behest of the New York investigative agents, who were governed by Second Circuit law.

was apprised of the relevant conduct, so that the magistrate was able to determine whether any predicate illegality precluded issuance of the warrant . . . invoking the good faith doctrine does not launder the agents' prior unconstitutional behavior . . . [and instead] reaffirms *Leon*'s basic lesson: that suppression is inappropriate where reliance on a warrant was objectively reasonable." *United States v. Ganias, 824 F.3d 199, 223 (2d Cir. 2016)* (en banc).

That precisely describes the situation here. There is no suggestion that government agents concealed any relevant facts from Magistrate Judge Aaron. To the contrary, they disclosed precisely those facts that now lead this Court to conclude the **[*46]** initial border search was unlawful in their application for a warrant. In nevertheless in issuing the warrant, the Magistrate Judge implicitly (if erroneously) found that the underlying border search that resulted in a copy of Smith's phone was lawful or, at the very least, that probable cause independent of that search existed to search the copy. Nor is this a case where law enforcement "could not fail to have known" that their search was unconstitutional. *Reilly, 76 F.3d at 1281*. Rather, like the law enforcement agents in *Thomas*, at the time of the search in this case, "no court in this Circuit had held that" phone searches at the border "w[ere] unconstitutional." *Ganias, 824 F.3d at 223*.[14] Since the unconstitutionality of the search of Smith's phone was not obvious and law enforcement agents presented all relevant facts that might (and, in this Court's view, do) establish its unconstitutionality to a neutral magistrate, their subsequent reliance on the search warrant issued by that magistrate was objectively reasonable.

That does not quite settle the question, because of the significant length of time -- 38 days -- between the Government's March 2, 2021 search and copying of Smith's phone and its finally obtaining a warrant on April **[*47]** 9, 2021. In general, if law enforcement seizes personal property before obtaining a warrant and seeks a warrant after the fact, it must act "with diligence [in] apply[ing] for the warrant." *United States v. Smith, 967 F.3d 198, 205 (2d Cir. 2020)*. Law enforcement must act with "expediency in obtaining a search warrant to search seized evidence in order to avoid interfering with a continuing possessory interest for longer than reasonably necessary," and because "unnecessary delays [] undermine the criminal justice process in a more general way [by] prevent[ing] the judiciary from promptly evaluating and correcting improper seizures." Id. Here, however, Smith makes no argument concerning the length of the delay between the copying of his phone's contents on March 2 and the Government's obtaining a warrant for it on April 9, so the issue is plainly waived. And even if that were not the case, the Court would still conclude that the good faith exception entitles the Government to rely on the April warrant.

In determining whether a particular delay between a seizure and the issuance of a warrant is reasonable, the Second Circuit has held that courts should consider "the following four factors . . . [1] the length of the delay, [2] the importance **[*48]** of the seized property to the defendant, [3] whether the defendant had a reduced property interest in the seized item, and [4] the strength of the state's justification for the delay." *Id. at 206*. The Government's delay here was plainly significant, since the Second Circuit has already held that a one-month delay (which is slightly shorter than the delay at issue here) "well exceeds what is ordinarily reasonable." *Id. at 206*. However, unlike in the typical case of delay following a warrantless seizure, Smith was not actually deprived of his use of his phone or the data stored on it, since the Government returned the original to him after it copied its contents. That makes this a different case from the Second Circuit's decision in *Smith*, where the police had seized a suspect's iPad, thereby depriving its owner of its use. Id.

Moreover, as in *Smith* itself, finding that the Government waited too long to seek a warrant would not necessarily justify excluding the results of its post-warrant search of the seized contents. How to think about the storage of forensic copies of a device containing digital data -- and the extent of the intrusion on a person's privacy interests resulting from the storage of such copies -- **[*49]** is a relatively novel question. In *Ganias*, the Second Circuit concluded that law enforcement acted in good faith where it obtained a warrant to seize and search a person's computer hard drives, made and retained forensic copies of the hard drives for several years, and ultimately searched those copies years later for information that was not responsive to the original warrant that led to the creation of the forensic copies. *Ganias, 824 F.3d at 225*. To be sure, there the Government was acting in reliance on a (years-earlier issued) warrant, id., whereas here the initial search and digital copying of the contents of Smith's phone was warrantless, but *Ganias*, which declined to settle

[14] This was true both in the Second Circuit, where the warrant was requested, and in the Third Circuit where the earlier search took place.

whether the Government's actions violated the *Fourth Amendment*, emphasized the unsettled and evolving nature of the law when it comes to copying and preserving electronic copies of the data on an electronic device. *Id. at 208-21*.

Moreover, while the Second Circuit in *Smith* clarified that a month was too long to wait in order to seek a warrant for a previously seized electronic device no longer available to its owner, id., it did not address a situation such as the one here, where the Government returned the actual phone and kept and (for the most part) searched the electronic **[*50]** copy after the warrant was issued. As in *Smith*, therefore, the Court is "not convinced that an objectively reasonable officer would have known that the delay [in obtaining a warrant] amounted to a violation of the *Fourth Amendment*." *967 F.3d at 213*.

Accordingly, for the foregoing reasons, the Court concludes that the good faith exception doubly applies here, so that while the Government's initial warrantless search of Smith's phone was unlawful, the results of that search (alongside the subsequent wiretap) should not be suppressed. Smith's motion to suppress is therefore denied.

III. Smith's motion to dismiss

Smith also moves to dismiss the indictment, contending that the Government's prosecution of him and the other defendants in this case was discriminatory. Smith Mem. 13-15. In support, he notes that he is black, the other defendants charged in this case are all either black or brown skinned, and that the affidavits submitted in support of the Government's warrant and wiretap applications refer to putative connections between Smith and other defendants with the Bloods gang. Id.; Smith Decl. ¶¶ 8-15, Dkt. 160. Smith also contends that many EMS companies are owned by white men whom the Government has declined to prosecute. **[*51]** Smith Decl. ¶ 14-15.

Because prosecution decisions are the "special province of the Executive," a "presumption of regularity supports [its] prosecutorial decisions," such that "absen[t] clear evidence to the contrary, courts presume that they have properly discharged their official duties." *United States v. Armstrong, 517 U.S. 456, 464, 116 S. Ct. 1480, 134 L. Ed. 2d 687 (1996)*. While that presumption may be overcome by evidence "that the decision whether to prosecute . . . [was] based on an unjustifiable standard such as race, religion, or other arbitrary classification," such evidence must be "clear" and demonstrate that the "prosecutorial policy had a discriminatory effect and . . . was motivated by a discriminatory purpose." *Id. at 465-66*. To establish a discriminatory effect based on race, a defendant "must show that similarly situated individuals of a different race were not prosecuted." *Id. at 465*.

Smith plainly fails to make the requisite showing. Smith has alleged only in very general terms that "owners of [EMS companies] and the people who worked for them -- almost entirely white men" without any gang connection also "settled their differences . . . by using threats of violence, violent kickbacks, or other illegal conduct." Smith Decl. ¶ 14. But while the indictment in this case lays **[*52]** out quite detailed allegations about Smith and his co-defendants' participation in a criminal enterprise that sought, inter alia, to impose a system of rules and rotation upon other EMS companies and use force to enforce that system, Indictment ¶¶ 6-10, Dkt. 2, Smith has not come forward with actual evidence of similar conduct by similarly situated white industry participants whom the Government has declined to prosecute. Similarly, Smith's only evidence of discriminatory intent is that the warrant and wiretap applications in this case referred to his and other defendants' putative connections with Bloods, but membership in the Bloods is certainly not itself any kind of protected status, and Smith has not explained how the Government's references to his or other defendants' putative connections to the Bloods demonstrate discrimination based on race or some other protected status. Accordingly, Smith's motion to dismiss the indictment is denied.

IV. Sequan Jackson's Motion to Suppress

Defendant Sequan Jackson also moved to suppress the results of a Title III wiretap of his and Smith's phones. As with Smith's motions to suppress and dismiss, the Court denied Jackson's motion by bottom-line **[*53]** order earlier this year. See Order, Dkt. 183.[15]

To obtain a Title III wiretap, the government must provide "a full and complete statement of the facts and circumstances relied upon by the application" to establish probable cause, and a "full and complete statement as to whether or not other investigative

[15] Jackson has since pled guilty to certain charges. See Order, Dkt. 202.

procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous." *18 U.S.C. §§ 2518(1)(b)-(c)*. These restrictions aim "to guarantee that wiretapping or bugging occur[] only when there is a genuine need for it and only to the extent that it is needed." *Dalia v. United States, 441 U.S. 238, 250, 99 S. Ct. 1682, 60 L. Ed. 2d 177 (1979)*. They require any "affidavit offered in support of a wiretap warrant [to] provide some basis for concluding that less intrusive investigative procedures are not feasible." *United States v. Lilla, 699 F.2d 99, 103 (2d Cir. 1983)*. At the same time, they do not require "that any particular investigative procedures be exhausted before a wiretap may be authorized." *Id. at 104*. Rather, "the statute only requires that the agents inform the authorizing judicial officer of the nature and progress of the investigation and of the difficulties inherent in the use of normal law enforcement methods." *United States v. Diaz, 176 F.3d 52, 111 (2d Cir. 1999)*. The Second Circuit has previously indicated that wiretaps will often prove **[*54]** necessary "in complex and sprawling criminal cases involving large conspiracies," given the difficulties to obtaining evidence in such cases. *United States v. Concepcion, 579 F.3d 214, 218 (2d Cir. 2009)*.

Jackson's primary argument is that the Government failed to establish that normal investigative procedures failed, would not succeed, or were too dangerous. Jackson Mem. 19-25, Dkt. 140. For instance, although the Government clearly gleaned extensive information from witness interviews (much of which formed the basis for its assertion there was probable cause for a wiretap), Clark Wiretap App. at 20-26, Jackson argued that the Government essentially stopped interviewing witnesses following the approval of the wiretap in order "to create the appearance of necessity" for its extension. Jackson Mem. 20. But just because the Government was able to make significant initial progress in its investigation with witness interviews does not mean that it could have continued to do so. As the Government cogently explained in support of its wiretap application, while its extensive witness interviews provided "important information" about how the alleged scheme was enforced as to victims, "victims have limited insight into the internal operations of the racketeering **[*55]** scheme . . . ." Clark Wiretap App. at 49. The Government further explained that because many of the victims it interviewed reasonably feared retaliation, their willingness to cooperate was often limited. Id. These explanations, along with the rest of the Government's wiretap explanation, more than satisfies the statutory requirement that the Government explain why further witness interviews "reasonably appear[ed] to be unlikely to succeed" in obtaining further evidence. 18 *§ 2518(1)(c)*.[16]

Jackson also points out that the Government was aware from its search of Smith's phone that First Response members communicated through an end-to-end encrypted WhatsApp chat which would not itself be observable through a wiretap. As such, Jackson suggests, that the Government should have sought cooperation from one of the many people included on one of the WhatsApp chats. But the wiretap application explains that while the Government obtained some information from cooperating witnesses, it was not aware of further confidential sources whom it believed would have relevant information and be willing to work with the Government. Clark Wiretap App. at 42-43. Of course, as Jackson notes, the Government could presumably **[*56]** have approached one of the participants in the WhatsApp group chats -- but such a move could just as easily have resulted in that participant tipping off Smith, Jackson, or the other targets of the investigation. Gov't Mem. at 23-24. Similarly, Jackson speculates that an undercover agent could potentially have gained access to the WhatsApp chats or otherwise obtained valuable information by appearing at the site of a fire and seeking to "blend" in with individuals from First Response as they showed up, Jackson Mem. 22, but that is pure speculation that would require undercover agents to show up at a moment's notice at the site of a fire, identify if EMS personnel who showed up were connected with First Response, and then somehow insinuate themselves into those persons' conversations. Such a speculative

---

[16] Jackson also suggests that because the Government has provided Jencks Act material for over 40 witnesses, it ultimately was able to obtain evidence from substantially more witnesses than the 16 it interviewed when applying for a wiretap -- indicating that there was more to be gained from witness interviews. Jackson Mem. 20-21. The Court is not convinced. For one thing, the fact that the Government produced Jencks Act evidence for more witnesses than it had apparently interviewed before seeking a wiretap does not itself raise any inference as to the quality of information provided by the additional witnesses. Furthermore, the wiretap itself likely produced new lines of inquiry, and the Government represents that additional witnesses became willing to speak to law enforcement after the charges in this case were brought. Gov't Mem. 23 n.3, Dkt. 164. So the fact that the Government ultimately interviewed more witnesses hardly defeats its explanation as to why, at the time it sought a wiretap, it was unlikely to obtain the information it needed from further witness interviews alone.

possibility is not enough to preclude issuance of a wiretap.[17]

The Court is similarly unpersuaded that there was anything deficient in the Government's representation in its warrant application that further physical surveillance would be insufficient, given the Government's description of its previous unsuccessful efforts to surveil the First Response office and monitor areas frequented **[*57]** by Smith and its explanation that because violence "occur[ed] at the site of fires or at other random locations," there was no practicable way to obtain needed evidence through physical surveillance. Clark Wiretap Application at 42-45.

Finally, Jackson argues that the wiretap never should have been approved because the Government knew from its search of Smith's phone that most of his text communications were sent by WhatsApp, and the Government's wiretapping technology allegedly would not allow it to pierce WhatsApp's end-to-end encryption. Jackson Mem. at 25-27. The Court is not persuaded. The fact that the majority of Smith's written messaging with large groups was through WhatsApp does not imply he used WhatsApp to make phone calls, and, indeed, the Government's wiretap application detailed several phone calls placed between Smith's cell phone and other suspects. Clark Wiretap App. at 38-41. Accordingly, the fact that Smith employed WhatsApp messaging did not mean the Government lacked reason to expect it would obtain valuable information from a wiretap.

The Court thus agrees with Judge Liman's determination that the Government adequately demonstrated that other investigative methods **[*58]** were not reasonably likely to succeed and that a wiretap was therefore necessary. Accordingly, Jackson's motion to suppress is denied.

[17] Jackson also implies that the Government's warrant application may not have been accurate because it describes an undercover HSI officer being sent to the scene of a fire in February 2021, Clark Wiretap Appl. at 41, even though the investigation that ultimately resulted in these charges was not formally opened until March 2021, id. at 14. Jackson Mem. 22 (arguing that "[t]his discrepancy raises the specter that there was, in fact, no actual use of an undercover officer"). But the Government explains that there were two overlapping investigations, and the February 2021 visit to the scene of a fire was conducted by officers associated with the earlier one. Gov't Mem. 26 n.5

V. Defendants' Dore and Lacewell's Motion to Sever

Finally, defendants Damon Dore and Rahmiek Lacewell moved under *Fed. R. Crim. Proc. 14* to sever their trial from Jatiek Smith's.[18] They argued that certain inculpatory evidence obtained during an interview Smith gave law enforcement might be admissible as to Smith but inadmissible as against them, that Smith is the most culpable of any defendant, and that Smith's pretrial behavior indicates he is likely to behave in a way during trial that will prejudice a jury against not just him but also moving defendants. See generally Mem. Supp. Mot. Sever, Dkt. 144. None of these arguments merit severance.

"A trial court has wide discretion in considering a motion to sever under *Federal Rule of Criminal Procedure 14*." *United States v. Gallo, 863 F.2d 185, 194 (2d Cir. 1988)*; see *Zafiro v. United States, 506 U.S. 534, 539, 113 S. Ct. 933, 122 L. Ed. 2d 317 (1993)*. To succeed on a motion to sever, the defendant must demonstrate "substantial prejudice," *United States v. Werner, 620 F.2d 922, 928 (2d Cir. 1980)*, such as might occur when evidence that would not be admissible as against the defendant seeking severance would be admissible against another and the evidence is of a sort that limiting instructions seem unlikely to cure any prejudice. *Zafiro, 506 U.S at 539*.

As to Smith's inculpatory **[*59]** statements, the Government argues that such statements are admissible against all defendants as co-conspirator statements, since, the Government contends, Smith gave the interview in question in order "to thwart law enforcement's investigation into those crimes by deflecting law enforcement's attention away from First Response and onto other EMS companies." Gov't Mem. at 13, Dkt. 164. The Court sees no need to resolve whether these statements really would have been admissible against defendants other than Smith for two reasons. First, even assuming moving defendants were right that these statements would be admissible against Smith but not them, they have not pointed to any

[18] Defendant Sequan Jackson originally joined this motion, although he subsequently withdrew from it. Dkt. 169. The motion was also joined by defendants Anthony McGee and Kaheen Small, who entered guilty pleas before the Court denied the motion. See Minute Entries dated 3/6/23 and 3/14/23. Lacewell and Dore have also subsequently pled guilty, although their pleas came after the Court denied their motion to sever by bottom-line order. See Order, Dkt. 183.

statements that would be so likely prejudicial that an appropriate limiting instruction would not adequately address their concerns. Further, the Government represents it has not even decided whether to seek to introduce any of these statements at trial, and that it would first resolve their admissibility via a motion in limine if it does choose to seek to introduce them.

As to defendants' argument that Smith is the most culpable defendant, the charges here -- racketeering and extortion conspiracy -- necessarily **[*60]** involve the actions of multiple individuals, with some likely more culpable than others. The Government represents that the evidence it intends to rely on to prove each defendant's participation in the conspiracy substantially overlaps. Even if moving defendants are right that their participation was less culpable than Smith's, the Court does not believe that such differential culpability does not by itself merits severance, absent some more particular showing that a joint trial is likely to prejudice a jury against moving defendants.

Finally, defendants' arguments about Smith's potential disruptiveness at trial are entirely speculative. They are based entirely on Smith's conduct in resisting arrest and in his refusal to leave a court cell block and return to jail following a conference earlier in this case. Defs. Mem. at 12, Dkt. 144. Mr. Smith has appeared at several court conferences and behaved in all respects appropriately while in Court; his apparent resistance to being returned to jail after one of these court appearances does not demonstrate that Smith will behave at trial in a way likely to cause prejudice to other defendants (especially since Smith himself will have every **[*61]** incentive at trial to present himself favorably to the jury). Accordingly, defendants Dore and Lacewell's motion to sever is denied.

VI. Conclusion

For the foregoing reasons, as indicated in its previous bottom-line order, the Court hereby reconfirms its denial of defendant Jatiek Smith's motion to suppress the results of the search of his phone and to dismiss the indictment, defendant Sequan Jackson's motion to suppress evidence obtained from Title III wiretaps, and defendants Dore and Lacewell's motion to sever their trial from Smith's.

SO ORDERED.

New York, NY

May 11, 2023

/s/ Jed S. Rakoff

JED S. RAKOFF, U.S.D.J.

End of Document